Walter Seböck, Maria Lukas (Hrsg.)

9. Sicherheitskonferenz Krems

27. Oktober 2011
Donau-Universität Krems

Walter Seböck, Maria Lukas (Hrsg.)

9. Sicherheitskonferenz Krems

„Auswirkungen der Kriminalität auf sicherheitsrelevante Fragestellungen“

Tagungsband der Konferenz 2011

27. Oktober 2011, Krems

© Donau-Universität Krems 2011

© Donau-Universität Krems

www.donau-uni.ac.at

Druck: Druckerei Berger

3580 Horn, Wiener Straße 80

ISBN 978-3-902505-24-8

VORWORT

Das Ziel der Sicherheitskonferenz der Donau-Universität Krems ist es, anhand aktueller Schwerpunkte die Entwicklungen im Sicherheitsbereich darzustellen, neue Konzepte zu präsentieren und Impulse zu setzen.

Waren bisher die Schwerpunkte der Konferenz primär im Bereich der IT- und Informationssicherheit orientiert, so wurde durch den Beschluss der Donau-Universität Krems, ein eigenständiges Zentrum für Infrastrukturelle Sicherheit sowie eine interdisziplinäre Plattform „Sicherheit“ zu errichten, die thematische Breite deutlich erhöht. Somit befasst sich das Zentrum für Infrastrukturelle Sicherheit an der Donau-Universität Krems sowohl in der Lehre als auch in der Forschung und Beratung mit den Themen der IT- und Informationssicherheit, Security und Safety sowie Fire Safety Management und Brandschutz.

Die interdisziplinäre Plattform „Sicherheit“ wird darüber hinaus die sicherheitsrelevanten Aspekte sämtlicher Schwerpunktbereiche der Fakultäten bündeln und darstellen. Dies umfasst wirtschaftswissenschaftliche, medizinische und bautechnische Sicherheitsthemen. Gleichzeitig soll diese Plattform eine Möglichkeit bieten, Forschungsergebnisse und Masterthesen zur Verfügung zu stellen und den inhaltlichen Austausch zwischen Studierenden, Wissenschaftlern und der Wirtschaft zu unterstützen.

Bereits aus dem skizzierten Themenumfang wird sichtbar, dass die Forschung und die Aktivitäten in diesem Bereich vielfältiger und relevanter Natur sind, da sie alle öffentlichen, wirtschaftlichen und individuellen Bereiche betreffen.

Es ist festzustellen, dass, wie in allen anderen Bereichen auch, die Ursachenforschung den größten Anteil an der Problemlösung trägt, aber dazu Maßnahmen erforderlich werden, die in ihrer Komplexität schwer überschaubar sind.

Das Regulativ, Technologien oder Gesetzeslagen zu adaptieren, bietet sich folglich als Problemlösung an, die aber immer nur kurzfristig wirkt. Bei der Betrachtung der Sicherheitsprobleme erscheint unmittelbar die Vermutung, dass diese oft technisch bedingt und daher auch nur technisch lösbar wären; dies führt allerdings auf eine rein technische Detailebene. Als Lösungsszenario diverser Probleme scheint dies das einfachste zu sein, da es eine rationale Betrachtung unterstützt und ein klar nachvollziehbares Ursache-Wirkungsprinzip unterstellt. Damit können die Probleme zwar temporär, nicht aber grundsätzlich gelöst werden. Beginnt man,

die Gründe und Ursachen für Sicherheitsprobleme zu analysieren, wird die Eindimensionalität des technikorientierten Ansatzes sichtbar, da das menschliche Handeln keine Berücksichtigung findet. Dieses Handeln ist aber in vielen Fällen der Auslöser für Sicherheitsprobleme.

Sicherheit setzt nun also nicht nur technische Schutzmaßnahmen voraus, sondern auch das richtige Bewusstsein von MitarbeiterInnen bzw. handelnden Personen, was wiederum bedeutet, dass die Sicherheitsmaßnahmen bekannt und vertraut sein müssen, damit die Sicherheit lebbar gemacht werden kann.

Der Schwerpunkt der diesjährigen Konferenz, Cyber Security – Cyber Crime betrifft mittlerweile nicht nur einzelne Nutzer. Laut Bundeskriminalamt wurden bereits im ersten Halbjahr 2011 um 10% mehr IT-Delikte gegenüber 2010 angezeigt. Auch in der Cyber Security wirkt der technikorientierte Ansatz den Bedrohungen zu eindimensional entgegen. Mit einer ganzheitlichen Betrachtung und Erforschung dieser Bedrohungsszenarien und der Gegenstrategien, scheint die Erfolgsaussicht ungleich größer. Bewusstseinsbildung steht hier an prominenter Stelle. So trägt auch diese Konferenz zur aktuellen Cyber Security - Kampagne in Österreich bei, um diese Problematik noch intensiver zu thematisieren.

Dieser Tagungsband sowie die Konferenz 2011 sollen eine aktuelle Bestandsaufnahme über die verschiedenen Bereiche von Cyber Security, Cyber Crime sowie architektonische Sicherheitsplanung bieten und von den neuesten Forschungsergebnissen der Donau-Universität Krems und ihrer Partner informieren.

An dieser Stelle bedanke ich mich herzlich bei allen Beteiligten an der Sicherheitskonferenz 2011, bei den AutorInnen, den Sponsoren und dem Organisationsteam für das Engagement.

Walter Seböck
Krems, September 2011

Programmkomitee:

- Univ.-Prof. Mag. Dr. Nikolaus Forgó, Leibniz Universität Hannover, Juristische Fakultät, Institut für Rechtsinformatik
- Mag. Edith Huber, zSPM, Donau-Universität Krems, Stabstelle für Forschungsservice und Internationales
- Mag. Dr. Peter Parycek MAS, Donau-Universität Krems, Department für E-Governance in Wirtschaft und Verwaltung
- Mag. Dr. Walter Seböck MSc, MBA, Donau-Universität Krems, Department für E-Governance in Wirtschaft und Verwaltung

Reviewerteam:

- Prof. Dr. Rüdiger Buchkremer, FOM Fachhochschule für Ökonomie und Management gemeinnützige GmbH, Fachbereich Wirtschaftsinformatik, Essen

- Dipl. -Ing. Dr. techn. Helmut Floegl, Donau-Universität Krems, Department für Bauen und Umwelt, Zentrum für Facility Management und Sicherheit

- Prof. (FH) Dipl.-Ing. Johann Haag, Fachhochschule St. Pölten GmbH, Studiengang IT-Security

- Dipl.-Betriebswirt Rolf von Rössing, International Vice President ISACA (Information Systems Audit and Control Association)

- Dipl.-Phys. Philipp Schaumann, Consultant, Experte für IT- und Informationssicherheit

- Prof. (FH) Univ.-Doz. Dr. Ingrid Schaumüller-Bichl, Fachhochschule Oberösterreich, Fakultät für Informatik, Kommunikation und Medien, Hagenberg

- Michael Zoratti, MSc, SecureLINE GmbH

Inhaltsverzeichnis

CYBER SECURITY – CYBER CRIME

Open Source Intelligence am Beispiel von KIRAS/MDL; Multimedia Documentation Lab **13**

Gerhard Backfried, Dorothea Aniola, Gerald Quirchmayr, Werner Winiwarter, Klaus Mak, H.C. Pilles, Christian Meurers, Martin Köstinger, Paul Wohlhart, Peter M. Roth

Cloud Speicherdienste als Angriffsvektoren **25**

Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, Edgar Weippl

Trust Center Controlled Code Access Security (TC³ AS) **39**

Grischa Schmiedl, Kerstin Blumenstein

Forensische Analyse von Smartphones **55**

Stefan Langeder, Matthias Schrattenholzer, Christopher Mallmann

Forensische Untersuchung multimedialer Daten **69**

Rainer Poisel, Simon Tjoa

Was wissen wir über Malware? **85**

Otto Hellwig

Von der Sicherheit im Kollektiv zum Schutz des Individuums: ein Paradigmenwechsel **101**

Rolf von Rössing

ARICHTEKTUR IN SICHERHEITSGESELLSCHAFTEN

Sicherheitsarchitektur und der Einfluss auf das Täterverhalten am Beispiel Bankraub **123**

Birgit Zetinigg

Die Morphologie der Sicherheitsgesellschaft: Architektonische Antworten in der Kriminologie **135**

Günter Stummvoll

CYBER SECURITY – CYBER CRIME

OPEN SOURCE INTELLIGENCE
AM BEISPIEL VON KIRAS/MDL
Multimedia Documentation Lab

Gerhard Backfried, Dorothea Aniola
Gerald Quirchmayr, Werner Winiwarter
Klaus Mak, H.C. Pilles, Christian Meurers
Martin Köstinger, Paul Wohlhart, Peter M. Roth

Dieses Dokument beschreibt das Multimedia Documentation Lab (MDL), ein System, welches eine große Menge multimedialer Daten, die typischerweise von Open Sources in einer unstrukturierten Form und in verschiedenen Formaten gesammelt werden, in Echtzeit verarbeitet. MDL ist ein Werkzeug für die Lagebild-Erstellung und Risikobewertung. Es erlaubt die Integration von Multimedia-Content in die Analyseprozesse für sicherheitsrelevante Problemstellungen.

1 Einleitung

Eine wesentliche Voraussetzung für die Arbeit von Entscheidungsträgern ist es, qualitätsgesicherte Information zur richtigen Zeit am richtigen Ort bereit gestellt zu bekommen. Dies trifft auch auf den Bereich der öffentlichen Sicherheit zu. Nur durch optimierte Informationsbereitstellung und –verarbeitung können Risken und Bedrohungen, etwa durch Organisierte Kriminalität, Terrorismus und im Katastrophenschutz effizient verringert werden. Hatten staatliche Behörden in der Vergangenheit einen signifikanten Informationsvorsprung, gewinnen heute Informationen in öffentlich zugänglichen Systemen für die Unterstützung bei der Entscheidungsfindung immer mehr an Bedeutung. Prominente Beispiele dafür sind das Erdbeben in Haiti oder die Nuklearkatastrophe in Fukushima, wo die Regierung zugibt, sich auf öffentliche Quellen gestützt zu haben und vom Kraftwerksbetreiber nicht entsprechend informiert worden zu sein.

Traditionell werden Medieninhalte wie Text, Animation, Audio und Video entweder isoliert oder als Multimedia-Dokumente betrachtet. Eine Vernetzung von Dokumenten bleibt dabei, wie großteils in der Informationsanalyse üblich, auf Links und Verweise, wie wir sie aus Hypertext-Systemen kennen, beschränkt.

Die inhaltliche Vernetzung stellt nach wie vor eher die Ausnahme dar.

Open Source Intelligence, die Suche nach und Analyse von Information in und aus frei verfügbaren Quellen, ist aufgrund des vorhandenen Volumens an Information in der Lage, immer besseren Input zu liefern. Entscheidende Voraussetzung für den Erfolg der Open Source Intelligence ist allerdings die Möglichkeit, die für eine bestimmte Entscheidungssituation relevante Information zeitgerecht zu finden, zu analysieren und dabei unterschiedliche Medientypen integriert betrachten zu können. Darüber hinaus kann sie auch helfen, bestimmte Aspekte besser einzuschätzen, wie etwa die Stimmung der Bevölkerung in einem Katastrophengebiet oder sich abzeichnende Krisen. Zugleich wäre es gerade in Krisensituationen wie Naturkatastrophen extrem wichtig, vor Ort auf die nötigen *Informationssammler* zurückgreifen zu können, um ein entsprechendes Lagebild erhalten zu können. Obwohl bereits heute ein Großteil dieser Informationen über Social Media Networks geliefert wird, muss leider davon ausgegangen werden, dass sie weitgehend ungenutzt bleiben.

Wie wichtig die Verfügbarkeit und Verlässlichkeit der Informationsquellen und die Qualität der Information selbst sind, zeigt das Beispiel des Abdrehens der USS Ronald Reagan vor Japan. Ohne verläßliche Information über die Ausbreitung des in Fukushima austretenden radioaktiven Materials war es unmöglich, die Sicherheit der Besatzung zu garantieren. Daher war ab einem gewissen Zeitpunkt eine Fortsetzung des Rettungseinsatzes nicht mehr zu verantworten.

Die Aufgabe, in einem stetig ansteigenden Informationsfluss, insbesondere multimedialer Inhalte in zahlreichen Sprachen, relevante Informationen zur Entscheidungsfindung aufzubereiten, wird zu einer interdisziplinären Herausforderung für Organisationen jedweder Art.

In MDL wird die Aufbereitung und Durchsuchbarkeit, sowie die Verteilung und Analyse von mehreren Informationsarten durch einen modulartigen Aufbau des Systems ermöglicht. So können Informationen und Informationsverweise aus Text-, Audio- und Video-Quellen in unterschiedlichen Variationen und Sprachen (wie auch hinsichtlich Qualität und Format) zugänglich gemacht werden. Die Ergebnisse stehen auf einem Multimedia-Server jederzeit zur Verfügung und können analysiert und visualisiert werden. Auch Benachrichtigungen können ausgesandt werden.

Neben der bisherigen Möglichkeit, Textdokumente effizient zu verarbeiten, sollen nun auch *Rich-media* Inhalte verarbeitet und zur Erstellung eines aktuellen Lagebildes herangezogen werden können. Diese heterogenen Inhalte (Radio, TV, Web-Sites, RSS-Feeds, Blogs, Wikis, Social Media …) müssen in einer Vielzahl von Sprachen, aus unterschiedlichen Quellen und in Echtzeit konstant zur Verfügung stehen. Über Ontologien oder Terminologie-Frameworks sollen Inhalte semantisch verknüpft und somit auffindbar gemacht werden.

Letztendlich soll ein Demonstrator entwickelt und zur Verfügung gestellt werden, in dem alle Systemmodule dem Stand- der -Technik entsprechen und mit existierenden Infrastrukturen und vorbereiteten Schnittstellen in bereits vorhandene Systeme integrierbar sind.

Im vorliegenden Dokument beschreiben die Autoren das MDL-System stellvertetend für jene Ansätze, die entwickelt werden, um frei verfügbare Information für Analysten und Entscheidungsträger effizient nutzbar zu machen.

2 Systembeschreibung

MDL besteht aus mehreren Modulen und Technologien in Komponentenform. Mit diesen Komponenten gemeinsam werden eine Reihe von Toolkits für die Endanwender bereit gestellt, so dass das System in einer sich ändernden Umgebung rasch und autonom erweitert und flexibel angepasst werden kann.

Die Inhalte finden über einen sogenannten Feeder Eingang in das System und werden dabei bereits verschiedenen Prozessen unterzogen. So wird beispielsweise Multimedia-Inhalt in Audio- und *Video-Tracks* gespalten. Für Audio-Daten beinhalten diese Prozessschritte die Segmentierung des Audiosignals, Aufteilung in sprachliche und nicht-sprachliche Segmente, Erkennung von Sprachen sowie textbasierte Verarbeitung der aus der Spracherkennung resultierenden Wortsequenzen.

Text-Inhalte werden normalisiert bevor sie den Prozessen der Erkennung von Named Entities (Named Entity Detection, NED) und der Themenerkennung (Topic Detection, TD) zugeführt werden.

Die aus diesem Prozess resultierenden Ergebnisse der einzelnen Verarbeitungsschienen liegen in einem proprietären XML Format oder in MPEG-7 vor und werden am Ende der Verarbeitungsvorgänge zusammen geführt (Late Fusion). Die XML-Dateien werden zusammen mit einer komprimierten Version der originalen Media Dateien auf den Media Mining Server (MMS) hochgeladen, wo sie durchsuchbar und für die Visualisierung einsetzbar sind.

Die Gesamtarchitektur des MDL-Systems basiert auf einer Server-Client Lösung und erlaubt die Entwicklung von unterschiedlichen Komponenten und Technologien auf unterschiedlichen Plattformen und Rechnern (allerdings sind nicht alle Komponenten multi-platform fähig). Mehrere Feeder, Indexer und Server (die entsprechend MMF, MMI und MMS genannt werden) können zu einem Komplettsystem kombiniert werden. *Abbildung 1* bietet einen Überblick der Gesamtarchitektur mit den einzelnen Komponenten des MDL Systems und deren Interaktion.

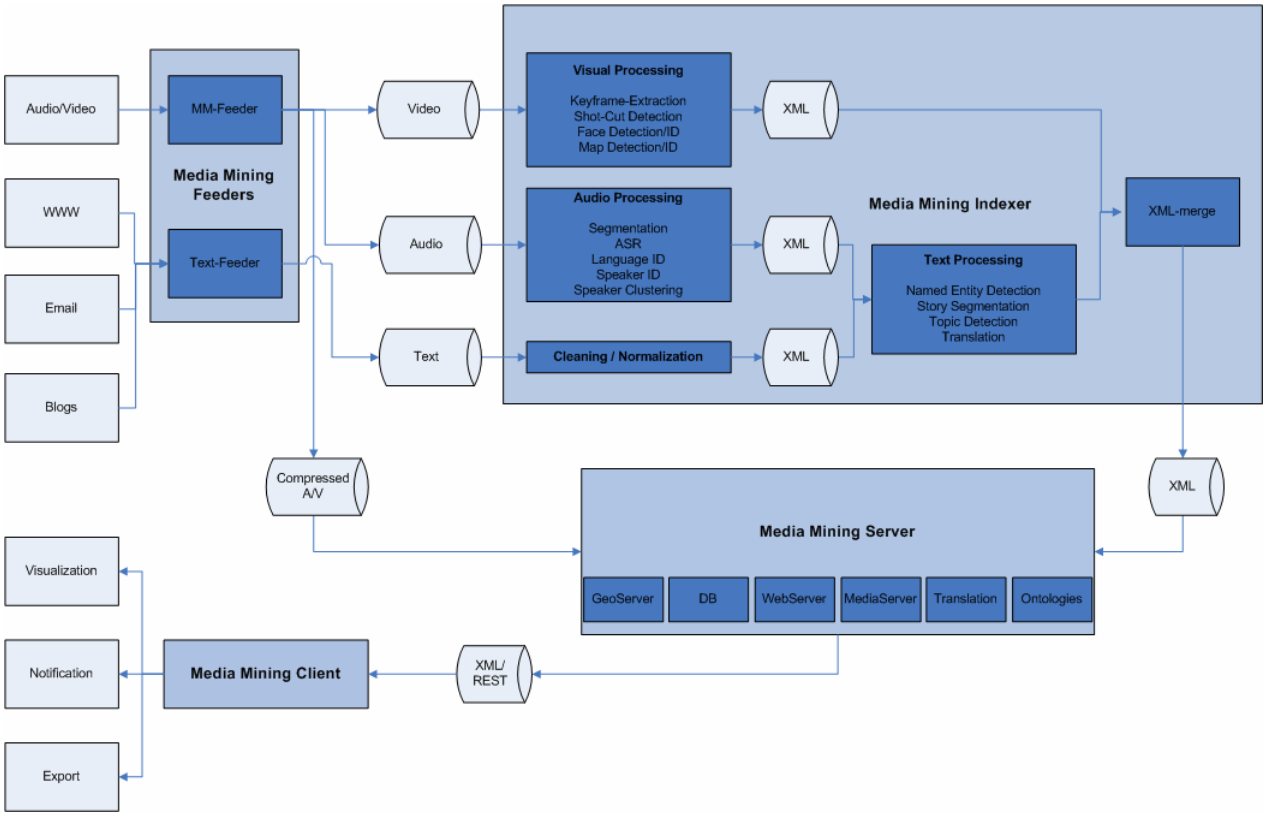


Abbildung 1 Gesamtarchitektur des MDL Systems

2.1 Feeder

Feeder stellen die Schnittstellen des MDL-Systems zur externen Umgebung dar. Für Audio oder Audio/Video-Input können diverse Formate von externen Quellen importiert und von Sub-Komponenten verarbeitet werden. Um textuellen Input (etwa Daten von Web-Seiten, Feeds, Emails oder Blogs) zu verarbeiten, kommen unterschiedliche Feeder zur Anwendung, welche die Daten von diesen Quellen extrahieren und sie an die Textverarbeitungskomponenten weiterleiten.

2.1.1 Multimedia Feeder (MMF)

Dieser Feeder basiert auf dem Direct Show Framework von Microsoft und kann eine Vielzahl von Quellen und Formaten verarbeiten. Die Daten werden hierbei auch re-enkodiert, um Windows Media Dateien zu erzeugen. Diese werden auf den Media Mining Server (MMS) hochgeladen, wo sie für spätere Suchvorgänge und Abfragen verwendet werden. Der Audio-Kanal wird an den Media Mining Indexer zur weiteren Verarbeitung weitergeleitet. Der Video-Kanal wird durch eine Reihe visueller Komponenten verarbeitet.

2.1.2 Text Feeder

Text Feeder stellen spezielle Komponenten dar, welche textuelle Informationen aus spezifischen Quellen extrahieren und diese an den Media Mining Indexer (MMI) weiterleiten. Zwei beispielhafte Text Feeder sind der Web-Collector (für die Verarbeitung von Web-Seiten, News-Feeds oder Blogs) und der Email-Collector (für die Verarbeitung von Emails und deren Attachments). Der resultierende Text wird bereinigt, tokenisiert und anschließend an die Text-Verarbeitungskomponenten des MMI weitergeleitet. Text Feeder können an spezielle Eingangsdaten angepasst werden (*customized Feeder*).

2.2 Media Mining Indexer (MMI)

Der MMI stellt das Herzstück der Verarbeitung von Audio und Text innerhalb des MDL Systems dar. Er besteht aus Technologien, als Komponenten verpackt, welche eine Reihe von Analyseschritten von Audio- und Text-Daten durchführen. Die Verarbeitungsresultate werden hierbei durch Anreicherung von XML-Strukturen kombiniert. Komponenten, um eine Vielzahl von Sprachen verarbeiten zu können, stehen bereits mittels MMI zur Verfügung. So ist beispielsweise die automatische Sprachverarbeitungskomponente bereits für über ein Dutzend Sprachen einsetzbar. Als Teil des MDL-Projektes wurde ein Modell zur Verarbeitung von Mandarin-Chinesisch entwickelt.

2.2.1 Segmentierung

Nach initialer Konvertierung durch den Feeder wird das Audio-Signal klassifiziert und segmentiert. Weitere Normalisierungs- und Konversionsschritte werden im Rahmen dieser Verarbeitung angewandt, wodurch das Audio-Signal in eine Sequenz homogener Abschnitte unterteilt wird. Die entstandenen Segmente stellen die Bausteine für alle weiteren Audio-Verarbeitungsschritte dar. Im Rahmen der Segmentierung kommen Modelle von sprachlichen- wie auch nicht-sprachlichen (z.B. Atemgeräusche, Lachen,...) Lauten zur Anwendung, um den optimalen Segmentierungspunkt zu ermitteln [1]. Die Segmente werden in Bezug auf ihren Sprachinhalt untersucht. Es werden ausschließlich Segmente, welche eine ausreichende Menge an Sprache enthalten, zur weiteren Verarbeitung herangezogen.

2.2.2 Sprechererkennung (Speaker-ID, SID)

Die Sprechererkennung wird auf die durch die Segmentierung erzeugten Abschnitte angewandt, wobei ein Set von vordefinierten Sprecher-Modellen eingesetzt wird. Diese Modelle umfassen typischerweise eine Reihe von Personen des öffentlichen Interesses. Sollte die Identität eines

Sprechers nicht festgestellt werden können, so versucht das System zumindest das Geschlecht des Sprechers zu identifizieren. Daten desselben Sprechers werden zusammengefasst und mit einer eindeutigen ID gekennzeichnet [2].

2.2.3 Automatische Sprachverarbeitung (Automatic Speech Recognition, ASR)

Die Spracherkennungskomponente wurde für große Vokabulare und sprecher-unabhängige, mehrsprachige Erkennung in Echtzeit entwickelt. Die Erkennung erfolgt hierbei in mehreren Schritten. In jedem Schritt kommen dabei genauere und komplexere Modelle zur Anwendung, die Zwischenresultate liefern und diese jeweils verfeinern und erweitern, um ein finales Transkript zu erzeugen [3]. Schließlich werden Verfahren der Textnormalisierung und sprachabhängige Verarbeitungsschritte [4] angewandt und das eigentliche Resultat des Spracherkenners in einem proprietären XML Format erzeugt. Der Spracherkenner verwendet eine zeit-synchrone, mehrphasige Suche, in welcher Gauss'sche Mixture Models, kontext-abhängige Phonemmodelle, und Wort- sowie Sub-wort basierte N-gram Sprachmodelle eingesetzt werden. Der Erkenner selbst ist sprachunabhängig und kann mit einer Vielfalt an Modellen in verschiedenen Sprachen und Bandbreiten betrieben werden.

2.2.4 Sprachenerkennung (Language ID, LID)

Sprachenerkennung wird auf Audio-Dateien angewandt, um die Sprache des Audio-Dokumentes zu identifizieren und ein für die Verarbeitung passendes Sprach-Modell zu wählen. Sie wird für Text-Dateien angewandt, damit adäquate Text-Verarbeitungsschritte gewählt werden können (oder eine entsprechende Verarbeitung im Rahmen des LMT bewirkt werden kann).

2.2.5 Text-Technologien

Text -Technologien werden entweder auf das Resultat der Spracherkennung oder auf dem Resultat der Text-Normalisierungsschritte angewandt. Normalisierung inkludiert die Vor-Verarbeitung, das Säubern (*cleaning*) und die Tokenisierung textueller Daten. Weiters werden sprachspezifische Schritte, so wie die Verarbeitung von Zahlen, Komposita, Abkürzungen oder Akronymen, Text-Segmentierung und Normalisierung der Grapheme im Rahmen dieses Schrittes angewandt.

Die Erkennung von *Named Entities* (NED), wie etwa Namen von Personen, Organisationen oder geographischen Orten, sowie die Erkennung von Zahlen, wird auf dem Resultat der Spracherkennung oder alternativ auf dem Output der Text-Normalisierungskomponenten

durchgeführt [5]. Das NED-System basiert einerseits auf Mustern, andererseits auf statistischen Modellen, welche auf Worten oder Wort-Eigenschaften definiert sind. Die Verarbeitung erfolgt auch hier in mehreren Schritten.

Die Themen-Erkennungskomponente (Topic Detection, TD) klassifiziert in einem ersten Schritt Sektionen des Eingangstextes. Die Modelle, die hierbei zur Anwendung kommen, sind durch eine spezifische Themen-Hierarchie vorgegeben. Sektionen, welche aneinander grenzen und einander ähnlich sind (bzw. identisch sind), werden zusammengelegt und re-klassifiziert. Die Modelle, welche hierbei zur Anwendung kommen, basieren auf Support-Vector Machines (SVM mit Linearen Kernels) [6].

2.3 Toolkits

Im Moment stehen zwei Toolkits zur Verfügung, die es den Anwendern erlauben, Modelle selbständig ihren Anforderungen entsprechend zu entwickeln oder anzupassen.

LMT (Language Model Toolkit): dieser Toolkit erlaubt den Anwendern die Spracherkennungsmodelle anzupassen oder zu erweitern. So können etwa neue, und dem derzeitigen Geschehen angepasste Wörter in das Vokabular des Spracherkenners aufgenommen werden. Gleichfalls können Aussprachen oder Wortverwendungen an lokale Gegebenheiten angepasst werden.

SIDTK (Speaker ID Toolkit): dieser Toolkit ermöglicht Anwendern die Sprechererkennungsmodelle zu erweitern oder neue Modelle zu erstellen.

Eine Anpassung und Erweiterung der Named-Entity Modelle durch den Anwender ist ebenfalls möglich.

2.4 Visuelle Informationsverarbeitung

Neben der Verarbeitung von Audio-Daten bietet MDL weiters die Möglichkeit Videodaten zu verarbeiten bzw. aus diesen Informationen zu extrahieren. Insbesondere sind das Detektieren bzw. das Erkennen von Personen (Gesichtern) und (geopolitischen) Karten von Interesse. Als kritisch, insbesondere für die Wahl der Methoden, muss in diesem Zusammenhang die Tatsache gesehen werden, dass Video-Streams oft mit starken Kompressionsartefakten behaftet sind oder mangelnde Auflösung aufweisen. Trotz dieser Einschränkungen müssen in Echtzeit akkurate Ergebnisse erzielt werden. Bevor die eigentlichen Schritte durchgeführt werden können, ist es notwendig kohärente zusammenhängende Videosequenzen zu extrahieren [7]. Sobald diese vorliegen, können alle weiteren Verarbeitungsschritte durchgeführt werden, die im Folgenden genauer beschrieben sind.

2.4.1 Gesichtsdetektion und –erkennung

Um in den Videodaten Gesichter von Personen erkennen zu können, müssen diese zunächst detektiert werden. Dazu wird in jedem Einzelbild des Video-Streams ein effizienter Gesichtsdetektor angewandt (z.B. [8]), der Positionen und Ausmaße aller im Bild vorhandenen Gesichter liefert. Danach werden diese in einem eigenen Erkennungsschritt mit Einträgen aus einer Datenbank bekannter Gesichter abgeglichen, wobei zunächst die Positionen charakteristischer und wiedererkennbarer Gesichtsmerkmale (wie z.B. Augen, Mundwinkel, ...) lokalisiert und durch robuste Beschreibungen (*Histogram of Oriented Gradients, Gabor Wavelets*) dargestellt werden.

Um eine vollständige Suche zu vermeiden, werden gelernte Modelle verwendet (z.B. *Support Vector Machines*), die eine effizientere Klassifikation ermöglichen. Dazu sind allerdings annotierte Trainingsdaten notwendig, die in der Praxis schwer zu erhalten sind bzw. ist dies mit einem großen manuellen Aufwand verbunden. Um diesen zu reduzieren, kann das System selbständig neue Gesichter von unbekannten Personen aufnehmen [9]. Dazu werden aus mit dem Video assoziierte Informationen (z.B. Teletext) oder mittels OCR (*Optical Character Recognition*) erkannte Texteinblendungen verwendet, um automatisch die Identität von Personen zu ermitteln.

Da nicht alle Ansichten eines Gesichts für eine präzise Erkennung geeignet sind (z.B. Profilansichten oder auch stark nach vorne oder hinten geneigte Posen) wird eine gefundene Person durch das Video hindurch verfolgt und es werden Einzelbilder generiert, die sie aus unterschiedlichen Blickwinkeln zeigen. Um diese so genannten *Face-Tracks* zu erhalten, werden individuelle Detektionen, die in einem zeitlichen und räumlichen Zusammenhang stehen, über Bewegungsinformation (*Optical Flow*) miteinander verknüpft.

2.4.2 Kartendetektion und –erkennung

Um geopolitische Karten in Nachrichtensendungen detektieren und in weiterer Folge erkennen zu können, wird ein dreistufiges Verfahren angewandt. Als erster Verarbeitungsschritt werden rechteckige Regionen bestimmt, die möglicherweise eine Karte enthalten. Dazu wird eine klassische *Hough Transformation* [10] berechnet, um horizontale und vertikale Linienzüge zu extrahieren. Danach werden die so ermittelten Regionen durch lokale visuelle Deskriptoren wie Farbhistogramme (LAB, RGB), -mittelwert, -varianz und Grauwertableitungen beschrieben und mit mit einem effizienten Klassifikator - *Extremely Randomized Forest* - (ERF) [11] gelernt. In der Testphase werden so Regionen, die mit sehr hoher Wahrscheinlichkeit keine Karten aufweisen, zurückgewiesen. Die verbleibenden Regionen werden hingegen einer detaillierten Analyse unterzogen.

Diese verbindet hierarchisches *Shape Matching* mit Texterkennung. Anschaulich wird hierbei verglichen, ob die in einer Region vorkommenden Konturen (z.B. Länderumriss) mit der

Kartenbeschriftung (z.B. Ländername) übereinstimmen. Textuelle Hinweise etwa auf Länder oder Städtenamen bieten direkten Rückschluss auf die Lage. Konturen von Subregionen (z.B. Provinz- oder Länderumriss) helfen zu disambiguieren, ob die Region wirklich eine Karte darstellt, oder fälschlicherweise als solche eingeordnet wurde. Weiters ist es so möglich Karten zu erkennen, die keine Beschriftung aufweisen oder Fälle abzudecken, in denen die Texterkennung fehlschlägt. Für die Detektion selbst werden mittels eines Segmentierungsbaumes [12] aussagekräftige Konturen von Subregionen bestimmt. Die dabei entstehenden Regionen werden mit der *Global Administrative Areas* (GADM)[1] Datenbank abgeglichen.

2.5 Media Mining Server (MMS)

Der Media Mining Server umfasst den eigentlichen Server, welcher zur Speicherung von XML und Multimedia-Dateien verwendet wird, wie auch ein Set an Tools und Schnittstellen, anhand derer der Inhalt der Datenbank abgefragt und aktualisiert werden kann. Sämtliche Interaktion mit dem MMS auf Seiten des Anwenders findet über den Media Mining Client (MMC) statt.

2.5.1 Media Server

Der Server stellt Speicherplatz für XML, Indices, Audio und Video-Dateien zur Verfügung. Er basiert auf dem Oracle 11g Datenbanksystem, welches sämtliche Such- und Analysefunktionalitäten zur Verfügung stellt. Die *Semantic Technologies* von Oracle stellen hierbei die Basis für alle ontologie-relevanten Funktionalitäten innerhalb von MDL zur Verfügung.

2.5.2 Ontologien

Ein Ontologie-Modell in MDL wird durch eine Reihe von Konzepten, Instanzen und Beziehungen definiert [13]. Sie stellen einen zentralen Knotenpunkt innerhalb des Systems dar und erlauben die Verknüpfung von Informationen, welche aus unterschiedlichen Sub-Systemen stammen [14]. Übersetzungen sind mit Konzepten der Ontologie verknüpft, wodurch eine konzept-basierte Übersetzung möglich ist. Während der Suche können Ontologien eingesetzt werden, um Suchkriterien zu erweitern oder einzuschränken. Das Netzwerk von Konzepten kann zu diesem Zwecke navigiert und eingesetzt werden. Verwandte Konzepte können aufgrund der strukturellen Information aus der Ontologie angezeigt und untersucht werden. Eine geographische Ontologie wurde bereits entwickelt und kann nun als Basis weiterer Entwicklungen verwendet werden. Weitere Ontologien, insbesondere im Gebiet der Naturkatastrophen (Überflutungen) befinden sich in Entwicklung. Im finalen System soll es möglich sein, Ontologien, welche mit externen

[1] http://www.gadm.org/

Werkzeugen entwickelt wurden (etwa mittels Protégé) auf einfache Weise zu importieren [15].

2.5.3 Übersetzung

Unterschiedliche Arten von Schnittstellen zu Übersetzungswerkzeugen werden von MMS zur Verfügung gestellt [16]. Parallel-Übersetzungen können bei Upload auf den MMS durch Zuhilfenahme von externen Übersetzungssystemen generiert werden. Weiters werden Wort-für-Wort Übersetzungen sowie eine Schnittstelle für menschliche Übersetzer zur Verfügung gestellt. Übersetzungen werden sowohl bei Suchen wie auch zur Visualisierung herangezogen.

2.6 Media Mining Client (MMC)

Der MMC stellt generell die Benutzerschnittstelle für Suche, Visualisierung, Updates und sämtliche Interaktion mit dem MMS dar. Benutzer können Abfragen durchführen, Inhalte herunterladen, Übersetzungen anfordern und Kommentare zu den Inhalten hinzufügen. Abfragen können freitextlich oder mittels logischer Ausdrücke durchgeführt werden, wobei der zugrunde liegende Datenbestand selektiert werden kann. Abfragen können abgespeichert und später für automatische Notifizierungen genutzt werden, wenn Dokumente, welche der abgespeicherten Abfrage entsprechen, auf den Server geladen werden. Suchergebnisse werden analog der vom MMI erzeugten Struktur dargestellt. Zusätzliche Informationen, wie etwa die Namen der erkannten Sprecher, *Named Entities* oder detektierte Karten werden mit dem Transkript eines Audio-Dokumentes zusammen dargestellt. Sowohl einzelne Sektionen, wie auch das gesamte Dokument können bei Bedarf abgespielt werden.

2.6.1 Visualisierung

Visualisierung der Datenbestände, welche den Anwendern erlaubt, diese in verschiedenen Sichtweisen darzustellen, spielt in MDL eine besonders wichtige Rolle. Suchergebnisse und Zusammenfassungen können verschiedenartig visualisiert werden. Dies gestattet Benutzern, Daten und Sachverhalte aus unterschiedlichen Blickwinkeln zu betrachten und iterativ von generellen zu spezifischen Blickpunkten wechseln. Eine Globus-Ansicht erlaubt, Ereignisse mit Örtlichkeiten zu verbinden. *Named Entities* (NEDs) können durch einen Beziehungsgraphen miteinander in Verbindung gebracht werden oder durch einen Trendgraphen zeitlich betrachtet werden. Durch eine Cluster-Ansicht können *Entities* und Informationsquellen miteinander in Beziehung gesetzt werden.

Weiterführende Abfragen können aus allen Visualisierungsmechanismen abgesetzt werden. Dies erlaubt z.B. in einem ersten Schritt, Ereignisse geographisch zu betrachten und in weiteren Schritten - ausgehend von der geographischen Information - tiefergehende Analysen zu starten. Ontologien können im Rahmen der Suche verwendet werden, um Abfragen zu modifizieren oder

zu leiten. Informationen, welche aus Ontologien abgeleitet werden, können bei der Suche direkt Einfluss finden (etwa durch semantische Erweiterung von Suchbegriffen) sowie für die Resultatsdarstellung angewendet werden.

2.7 Crisis Room (CR)

Einen weiteren Client stellt der Crisis Room dar, welcher zur gleichzeitigen Beobachtung zahlreicher TV- oder Radio-Kanäle eingesetzt werden kann. Ein typisches Szenario umfasst dabei die Projizierung mehrerer TV Kanäle mittels Beamer, wobei eine Vielzahl von Layouts für die Darstellung der gewählten TV Kanäle möglich ist. Zusätzlich steht ein Arbeitsplatz zur Verfügung, welcher zur Interaktion mit dem CR dient. Der CR erlaubt die kontinuierliche parallele Beobachtung des Auftretens von spezifischen Schlüsselwörtern und die gezielte Suche nach Stichworten. Das Auftreten eines Schlüsselwortes bewirkt dabei ein visuelles Feedback-Signal. Die Aufmerksamkeit des Benutzers wird auf einen konkreten Kanal gelenkt, wobei dieser nachfolgend auch zur Suche und für Playback verwendet werden kann. CR erlaubt folglich eine zeitnahe Analyse und Fokussierung auf relevante Themen und Ereignisse.

3 Status und Ausblick

Eine Vielzahl an Komponenten, wie etwa mehrere Feeder, Komponenten des MMS sowie sämtliche im Rahmen des MMI eingesetzten Komponenten sind bereits verfügbar und in Verwendung. Weitere Komponenten, beispielsweise zur visuellen Verarbeitung oder des MMS, befinden sich zur Zeit in Entwicklung oder sind als Prototypen verfügbar. Ein initiales System wurde beim Endanwender installiert und wird zu Evaluierungszwecken und für die Generierung von Feedback eingesetzt. Weitere Komponenten und Technologien werden schrittweise in die bestehende Installation integriert, um ein möglichst rasches Feedback zu erlauben.

Das MDL-System stellt ein Komplett-System entsprechend dem Stand- der- Technik im Bereich der Open Source Intelligence dar. Der finale Demonstrator wird sämtliche beschriebene Komponenten beinhalten. Um einen konstanten Informationsfluss zu gewährleisten, werden Feeders zur Beobachtung von TV Kanälen in einem 24x7 Modus eingesetzt werden. Diese werden Eingang in einen MMI finden, welcher seinerseits einen kontinuierlichen Eingangsstrom an Daten für den MMS erzeugt. In weiterer Folge werden Text-Feeder eingesetzt werden, um konstanten Input an textuellen Daten, etwa RSS-feeds oder Web-Seiten, zu liefern. Alle Verarbeitungsschritte sollen in Echtzeit und mit minimaler Verzögerung durchgeführt werden. Die Resultate aller Verarbeitungsschritte werden auf dem MMS und zum Export in die vorhandene Infrastruktur bereit gestellt. Es ist beabsichtigt, MDL als eine zentrale Komponente des existierenden SAC *(Situational Awareness Center*) Systems zu etablieren. Auch über den Kontext des

gegenständlichen Projektes hinaus wird MDL in einer Reihe von Anwendungsgebieten, wie etwa in der Bekämpfung der Organisierten Kriminalität oder bei der Terrorismusbekämpfung eingesetzt werden können.

Literatur

[1] LIU, D. und KUBALA, F., Fast Speaker Change Detection for Broadcast News Transcription and Indexing, Eurospeech, 1999.

[2] LIU, D. und KUBALA, F., Online Speaker Clustering, ICASSP, 2003.

[3] SCHWARTZ, R., NGUYEN, L. und MAKHOUL, J., Multiple-Pass Search Strategies, Automatic Speech and Speaker Recognition, 1996.

[4] HECHT, R., RIEDLER, J. und BACKFRIED, G., Fitting German into N-Gram Language Models, TSD, 2002.

[5] BIKEL, D., MILLER, S., SCHARTZ, R. und WEISCHEDEL, R., Nymble: High-Performance Learning Name-Finder, Conference on Applied Natural Language Processing, 1997.

[6] JOACHIMS, T., Text Categorisation with Support Vector Machines: Learning with many Relevant Features, in ECML, 1998.

[7] SMEATON, A.F., TABAN, R. und OVER, P., The TREC-2001 video track report, In Proc. Text Retrieval Conference, 2001.

[8] VIOLA, P. und JONES, M.J., Robust Real-Time face detection, Int'l Journal of Computer Vision, 57(2):137–154, 2004.

[9] WOHLHART, P., KOESTINGER, M., ROTH, P.M., und BISCHOF, H., Multiple Instance Boosting for Face Recognition in Videos , In Proc. DAGM Symposium, 2011 (to be published).

[10] HOUGH, P., Method and means for recognizing complex patterns, In USENIX Security Symposium, 1962.

[11] GEURTS, P., ERNST, D., und WEHENKEL, L., Extremely randomized trees, Machine Learning, 36(1):3–42, 2006.

[12] GU, C., LIM, J., ARBELAEZ, P., und MALIK, J., Recognition using regions, In Proc. Conf. on Computer Vision and Pattern Recognition, 2009.

[13] ALLEMANG, D. und HENDLER, J., Semantic Web for the Working Ontologist. Morgan Kaufman, 2008.

[14] DAVIES, J., GROBELNIK, M. und MLADENIC, D. (eds), Semantic Knowledge Management. Integrating Ontology Management, Knowledge Discovery, and Human Language Technologies, Springer-Verlag, 2009.

[15] Protégé Web-Site at Stanford University, http://protege.stanford.edu/, 2010.

[16] JURAFSKY, D. und MARTIN, J. H. Speech and Language Processing, Pearson, 2009.

CLOUD SPEICHERDIENSTE ALS ANGRIFFSVEKTOREN

Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner,
Markus Huber, Edgar Weippl

Während der letzten Jahre etablierte sich eine Vielzahl von Online File Storage Diensten. Während sich manche auf Basisfunktionalitäten beschränken bieten ausgereiftere Services auch Dienste wie gemeinsame Ordner („Shared Folder") für die Parallelnutzung durch mehrere Personen, die Möglichkeit zur Echtzeitzusammenarbeit, eine Minimierung des Datentransfers oder nahezu unbegrenzte Speicherkapazität.
Im Zuge dieses Artikels soll eine generelle Übersicht zu aktuellen Speicherservices im Internet geboten werden, sowie die Ergebnisse unserer Untersuchungen zu Dropbox als Beispiel einer populären Softwarelösung präsentiert werden. Schlussfolgernd aus unseren Resultaten konnten wir zeigen, dass Dropbox als Speicherort für urheberrechtlich geschützte Dateien aus Filesharingnetzwerken genutzt wird. Darüber hinaus ist es möglich über Dropbox unbemerkt unbegrenzt Daten zu speichern. Das Missbrauchspotential, so Daten zu verbergen, definieren wir als Online Slack Space. Abschließend zeigen wir mögliche Gegenmaßnahmen, um unsere Angriffe zu verhindern, und wie sie im Falle von Dropbox konkret implementiert werden könnten.

1 Einleitung

Viele innovative Speicherdienste wurden in den letzten Jahren vorgestellt, um Dateien auf zentralen Servern oder auf mehreren Rechnern verteilt im Internet zu speichern. Die gegenwärtigen Speicherservices folgen größtenteils einem einfachen Konzept und bieten ihren Nutzern recht elementare Funktionen. Vom technischen Standpunkt aus betrachtet, basieren die meisten dieser Dienste auf etablierten Protokollen wie FTP [28] oder WebDAV [22], einer Erweiterung des HTTP-Protokolls.

Mit Aufkommen des Cloud Computing und der gemeinsamen Nutzung von Ressourcen gewannen diese zentralisierten Speicherdienste an Relevanz und die Zahl der Nutzer stieg signifikant. Im Konzept des *Cloud Storage* können Festplattenkapazitäten oder Netzwerkbandbreite diese gemeinsam genutzten Ressourcen darstellen. Für die Betreiber dieser Services ist es naheliegend diese Daten nicht doppelt zu speichern, da es eine Vielzahl von identischen Dateien (wie z.B. Installationsdateien) gibt, die von mehreren Nutzern verwendet werden. Nachdem sowohl Datentransfer als auch Speicherbelegung für den Betreiber Kostenfaktoren darstellen, wird die

Tendenz zu einer Einschränkung überflüssig verbrauchter Kapazität, wie sie z.B. durch Mehrfachübertragung ein und derselben Datei entsteht, verständlich. Dropbox ist einer der größte Online Storage Service, der diesbezügliche Verfahren (z.B. Deduplikation) anwendet [24].

Aus der Sicherheitsperspektive erwachsen jedoch durch die gemeinsame Verwendung von Dateien gänzlich neue Herausforderungen. Die klare Abgrenzung von Nutzerdaten ist nicht im selben Maße durchführbar wie im klassischen Dateihosting und neue Methoden werden notwendig um sicherzustellen, dass in diesem Fundus gemeinsam genutzter Daten der Zugriff nur in autorisierter Form geschehen kann. Das ist unserer Auffassung nach die grundlegende Herausforderung für effiziente und sichere Cloud-basierte Speicherdienste. Themen wie unberechtigter Datenzugriff („Unauthorized Data Access“) oder ungewollter Informationsweitergabe („Information Leakage“) wurde in diesem Bereich aber noch kaum aufgearbeitet.

Unsere Vorschläge, um unautorisierten Zugriff auf Daten oder Information Leakage zuvorzukommen, sind nicht spezifisch für Dropbox, sondern sind für alle Online Speicherdienste von Relevanz die Deduplikation verwenden. Wir sind davon überzeugt, dass die Anzahl der Cloud-basierten Speicherdienste in näherer Zukunft enorm steigen wird.

Die wichtigen Punkte dieses Artikels sind:

- Die Funktionalität eines ausgereifteren Speicherdienstes im Detail darzustellen: Dropbox;
- Zu dokumentieren unter welchen Umständen unerlaubter Zugriff auf Daten möglich ist;
- Festzustellen ob Dropbox zur Speicherung urheberrechtlich geschützter Inhalte verwendet wird;
- *Online Slack Space* zu definieren und welche Probleme sich daraus für forensische Untersuchungen ergeben können
- Client- und serverseitige Gegenmaßnahmen zu formulieren, um die Sicherheitsrisiken für Nutzerdaten zu vermindern.

2 Hintergründe

In diesem Abschnitt werden die technischen Details und die von Dropbox umgesetzten Sicherheitsmaßnahmen behandelt. Im Rahmen dieses Artikels verwenden wir den Begriff „Cloud Computing“ wie definiert in [9]. Das beinhaltet alle Anwendungen auf die über das Internet zugegriffen wird und deren Hardware sich in einem Datenzentrum befindet, also nicht zwangsläufig unter der Kontrolle des Nutzers.

Im Folgenden beschreiben wir Dropbox und wichtige Sekundärliteratur zu den Speicherdiensten in der Cloud.

2.1 Dropbox

Seit seiner Markteinführung 2008 hat sich Dropbox zu einem der beliebtesten Cloud Storage Provider entwickelt. Dropbox hat 25 Millionen Nutzer und speichert mehr als 100 Milliarden Dateien, so der Stand von Mai 2011 [2], mit einem durchschnittlich geschätzten 5-minütlichen Zuwachs von 1 Million Dateien [3]. Dropbox dient vornehmlich als Speicherplatz für Online Backups, die über das Internet abrufbar sind. Eine auf dem jeweiligen Rechner installierte Software sorgt dafür, dass die Dateien in den spezifizierten Ordnern ständig mit den Servern synchronisiert werden und Änderungen auf den unterschiedlichen Geräten des Nutzers immer aktuell bleiben. Es besteht auch die Möglichkeit, mehrere Nutzer auf gemeinsame Ordner zugreifen zu lassen. Änderungen in diesen gemeinsamen Ordnern werden automatisch synchronisiert und in alle beteiligten lokalen Dropbox-Ordner überspielt. Der Großteil des Dropbox-Clients ist in Phyton programmiert.

Dropbox verwendet zur Dateiidentifikation nicht das herkömmliche Dateikonzept. Vielmehr wird jede Datei in 4 MB große Abschnitte („Chunks“) unterteilt. Fügt ein Benutzer eine Datei in seinem Dropbox-Ordner hinzu, berechnet die Software unter Verwendung des SHA-256-Hashalgorithmus die Prüfsummen (Hashwerte) für jeden dieser Abschnitte und überprüft, ob sich eventuell bereits eine Datei mit den entsprechenden Hashwerten auf dem Sever befindet. Ist dem nicht so, erhält der Client die Anweisung, die entsprechenden Chunks hochzuladen. Befindet sich die Datei bereits am Server, erfolgt kein Upload. Stattdessen wird die vorhandene Datei mit dem Dropbox-Account verlinkt. Dieser Ansatz erlaubt Dropbox Einsparungen hinsichtlich Transfer- und Speicherbelegungskosten, der Anwender wiederum profitiert vom rascheren Synchronisationsprozess. Zusätzlich finden weitere Techniken zur Steigerung der Effizienz Verwendung, z.B. Delta-Encoding, bei welchem nur die seit dem letzten Synchronisationsprozess modifizierten Abschnitte der Chunks übertragen werden. Die Wahrscheinlichkeit einer zufälligen Übereinstimmung der Prüfsummen unterschiedlicher Files ist verschwindend gering. Würden jedoch zwei unterschiedliche Dateien dieselben SHA-256 Hashwerte aufweisen, so wäre es einem Anwender möglich, auf Daten eines anderen Nutzers zuzugreifen, da die Datei die sich bereits auf dem Server befindet mit dem Account verknüpft werden würde.

Die Verbindung zwischen Client und Dropbox-Server wird über SSL gesichert. Die übertragenen Daten sind mit AES-256 verschlüsselt und werden im Amazons S3 Storage Service gespeichert, einem Teil des Amazon Web Services (AWS) [1]. Der AES-Schlüssel ist benutzerunabhängig und sichert die Daten nur während der Speicherung auf Amazon S3, die Sicherheit während der Übertragung basiert auf SSL. Unsere Untersuchungen zeigten, dass das Übertragungsprotokoll die

Daten direkt an Amazon übermittelt. Die Verschlüsselung selbst geschieht erst im Nachhinein, was nicht nur Fragen in Bezug auf Alternation und Speicherort der Schlüssel selbst offen lässt, sondern auch Zweifel in Bezug auf potentielle Zugriffsmöglichkeiten von Amazon auf diese Schlüssel aufwirft. Nach dem Upload erfolgt – zur Bestätigung des erfolgreichen Transfers – ein neuerlicher Abgleich des Hashwerts der eben hochgeladenen Datei und dem der Datei, die sich am Rechner des Nutzers befindet. Divergieren die Prüfsummen, wird der Transfer des jeweiligen Chunks wiederholt. Der offensichtliche Nachteil ist, dass der Server nur Werte bereits hochgeladener Chunks berechnen kann, nicht aber überprüfen kann ob der Client sich tatsächlich in Besitz der Dateien befindet, auf die er über eine Hashwert-basierte Datei-Abfrage zugreifen möchte. Der Client Software wird ungeprüft Vertrauen entgegen gebracht. Wie unsere Forschungsergebnisse zeigen, eine optimale Ausgangslage für zahlreiche Manipulationsmöglichkeiten!

Aufgrund des Aufschwungs im Bereich Cloud Computing stieg auch die Anzahl der konkurrierenden Anbieter. Die Hersteller der bekannten Betriebssysteme entwickelten Dienste, die sich mit den eigenen Produkten kompatibel zeigten, wohingegen sich kleinere Startups durch Betriebssystemunabhängigkeit oder ausgereiftere Sicherheitsmerkmale hervortun.

2.2 Sekundärliteratur

Relevante Forschungsarbeit konzentriert sich hauptsächlich darauf, ob sich der Cloud Storage Anbieter weiterhin in Besitz der Anwenderdatei befindet und ob diese möglicherweise vom Betreiber des Dienstes verändert wurde. Eine interessante Untersuchung zur allgemeinen Sicherheitsthematik von Cloud Computing findet sich in [30]. Ein Überblick von Angriffsszenarien und Sicherheitsmängeln wird in [17] geboten. Shachams Artikel [11] zeigt, dass es recht einfach ist die interne Infrastruktur von Cloud Storage Anbietern abzubilden. Darüber hinaus wurden sog. „co-location“ Angriffe beschrieben. Hierbei wird die Kontrolle über eine virtuelle Maschine übernommen, die sich auf derselben Hardware befindet wie das anzugreifende Zielsystem. Das ermöglicht in weiterer Folge Data Leakage und die Möglichkeit eines Side Channel-Angriffs auf die Virtual Maschine.

Frühe Publikationen [25, 14] behandeln unter anderem die Forschungsfrage, ob nichtvertrauenswürdige Dritte auf eine Datei zugreifen können, ohne dass diese im Vorfeld (komplett) von ihnen übertragen werden muss. Weiters wurden weitaus komplexere Protokolle vorgeschlagen um nachzuweisen dass der Server noch im Besitz der Datei ist [11, 12, 13, 20, 23, 29, 31, 32]. In einer aktuellen Publikation werden ähnliche Angriffe vorgestellt, allerdings ohne konkrete Implementierungen [24].

3 Unautorisierte Zugriffe auf Daten

In diesem Abschnitt stellen wir drei Angriffsszenarien auf Dropbox vor, um zu demonstrieren, wie ein unerlaubter Zugriff auf Daten erfolgen kann. Einzige Voraussetzung für die Angriffe ist, dass die Hashwerte der Dateien bekannt sind. Diese Angriffsmöglichkeiten sind jedoch nicht spezifisch für Dropbox sondern für alle Dienstleister die Deduplikation im Hintergrund einsetzen.

3.1 Hash Value Manipulation Angriff

Für die Berechnung des SHA-256 Hashwertes wird von Dropbox nicht die Phyton-eigene Hashlib-Bibliothek verwendet. Stattdessen wird die Kalkulation unter Einbeziehung von NCrypto [6], einer Wrapper Library für OpenSSL [18] durchgeführt. Dropbox-Clients für Linux und Mac OS X verwenden Bibliotheken wie NCrypto ohne sie vorher zu verifizieren. Wir veränderten den frei zugänglichen Quellcode von NCrypto dahingehend, dass die von OpenSSL berechnete Prüfsumme durch eine von uns gewählte ersetzt wurde. Der Dropbox-Client erkennt die Manipulation nicht als solche und übermittelt für jede neue Datei im lokalen Dropbox-Ordner den modifizierten Hashwert an den Server. Falls die Datei auf dem Server noch nicht vorhanden ist wird sie hochgeladen. Nach dem Upload erfolgt – zur Bestätigung des erfolgreichen Transfers – ein neuerlicher Abgleich des Hashwerts der eben hochgeladenen Datei und dem der lokalen Datei. Ausgehend von unserer Client-seitigen Manipulation können die Hashwerte nicht übereinstimmen und der Server wird eine neuerliche Übertragung anfordern, um einen offensichtlichen Übermittlungsfehler auszugleichen. Stimmen die Prüfsummen der Serverdatenbank mit der Berechnung des Clients jedoch überein erfolgt eine Verlinkung der jeweiligen Datei bzw. des Chunks mit dem Dropbox-Account. Aufgrund unserer vorangegangenen Prüfsummenmanipulation erhalten wir somit unberechtigterweise Zugriff auf Dateien. Dieser Angriff bleibt vor dem legitimen Nutzer vollkommen verborgen. Sind dem Angreifer die Hashwerte bekannt, eröffnet sich ihm so die Möglichkeit, Daten direkt vom Dropbox-Server herunterzuladen. Da keine Interaktion mit einem Benutzer nötig ist kann das Opfer diesen Angriff nicht entdecken oder verhindern, da keinerlei Zugriff auf dessen Rechner notwendig ist. Dieser Angriff wird aber auch vom Server nicht als solcher identifiziert, zumal er ja davon ausgeht, dass der Angreifer sich im Besitz der Datei befindet und diese nur seinem lokalen Dropbox-Ordner hinzugefügt hat.

3.2 Stolen Host ID Angriff

Wird eine Dropbox-Client-Applikation auf einem Computer oder Smartphone installiert, wird ein einmaliger Schlüssel vergeben, der das jeweilige Gerät mit dem Dropbox-Account des Benutzers verknüpft. Diese Host-ID wird unter Zuhilfenahme von Benutzername und Passwort vom Dropbox-Server individuell berechnet. Das bedeutet, dass die Authentifizierung von Client und User später

nicht über die Kombination von Benutzername und Passwort erfolgt, sondern über diese ID. Sobald Client und Host verbunden sind, ist keine neuerliche Anmeldung erforderlich, solange die Software nicht entfernt wird – eine augenscheinliche Sicherheitslücke. Denn ist der Angreifer (z.B. durch den Einsatz von Malware oder Social Engineering) erst in Besitz der Host-ID, erlangt er durch simples Ersetzen der eigenen ID Zugriff auf alle Daten des Opfers.

3.3 Direkter Download Angriff

Das Übermittlungsprotokoll zwischen Client-Software und Server basiert auf HTTPS. Die Client-Software kann Chunks über die URL https://dlclientXX.dropbox.com/retrieve (wobei XX durch fortlaufende Nummern ersetzt wird) anfordern, indem der SHA-256 Hash des Dateiabschnitts sowie eine gültige Host-ID als HTTPS POST Daten angegeben werden. Wie bereits erwähnt, fordert der Client Dateien über deren Hashwert an. Erstaunlicherweise ist für die Abfragemethode einer auf dem Dropbox-Server liegenden Datei nur die Kenntnis ihrer Prüfsumme sowie eine gültige Host-ID Voraussetzung. Es hat sich gezeigt, dass keinerlei Überprüfung erfolgt, ob der mit der Host-ID verlinkte Account bzw. dessen Benutzer tatsächlich in Besitz der angeforderten Datei ist. Wie wir später noch zeigen werden, werden von Dropbox kaum Daten gelöscht.

3.4 Erkennen von Angriffen

Zusammenfassend lässt sich sagen, dass ein Angreifer, der Zugang zum Inhalt der Client-Datenbank erlangt, alle Dateien die mit diesem Account verknüpft sind direkt vom Dropbox-Server laden kann. Dazu ist kein weiterer Zugriff auf das System des Geschädigten erforderlich, im einfachsten Fall ist überhaupt nur die Host-ID notwendig. Sollte sich das Interesse des Angreifers auf bestimmte Dateien beschränken so reicht zum Zugriff darauf die Kenntnis der entsprechenden Hashwerte aus. Findet eine der oben genannten Methoden Anwendung, ist der unerlaubte Zugriff für den tatsächlichen Besitzer der Dateien nicht ersichtlich.

Aus der Sicht des Cloud Storage Service Operators sind sowohl Stolen Host-ID Angriffe als auch der direkte Download Angriff bis zu einem bestimmten Grad nachweisbar. Dahingegen bleibt ein Hash-Manipulation-Angriff unerkannt, da diese Methode des unautorisierten Zugriffs den Anschein erweckt, der Angreifer würde sich bereits im Besitz der Datei befinden. Mögliche Gegenmaßnahmen beschreiben wir unter Abschnitt 6.

4 Angriffsvektoren und Online Slack Space

Folgender Abschnitt widmet sich Angriffstechniken die darauf abzielen, das Wirkungsprinzip von Cloud Storages generell auszunutzen. Beschrieben werden bereits bekannte Angriffsvektoren und diesbezügliche Umsetzungsmöglichkeiten mithilfe von Dropbox oder anderen Cloud Storage Services mit mangelhaften Sicherheitsvorkehrungen. Der Großteil zieht schwerwiegende Folgen nach sich und sollte im Gefahrenmodell dieser Services bedacht werden.

4.1 Online Slack Space

Der Upload von Dateien auf den Dropbox-Server ähnelt dem bereits beschriebenen Download über HTTPS. Der Upload eines Chunks über die Client-Software erfolgt nach Aufrufen von https://dl-clientXX.dropbox.com/store mittels Hashwert und Host-ID als HTTPS POST Daten, zusätzlich zu den eigentlichen Daten. Nach erfolgreichem Transfer erfolgt über eine weitere HTTPS-Anfrage eine Verlinkung von übertragener Datei und Host-ID und die neu hinzugefügten Dateien werden mit allen Geräten der Benutzers oder allen Accounts, die Zugriff auf diese Ordner haben, synchronisiert. Mit einem modifizierten Client ist es allerdings möglich, diesen Verlinkungsprozess zu unterbinden und unbemerkt unbeschränkt große Dateien hochzuladen, ohne dass dieses Datenvolumen vom Server als solches registriert wird und somit im Verborgenen weiterer Speicherplatz genutzt werden kann. Diese Sicherheitslücke haben wir als *Online Slack Space* bezeichnet, in Anlehnung an die forensische Methode Informationen im letzen Block von Dateien zu verbergen, die diesen Block nicht vollständig ausfüllen [21]. Doch anstatt Informationen im letzen Datenblock zu verbergen, geschieht dies hier unter Verwendung von Chunks, die nicht mit dem Benutzer-/Angreifer-Account verlinkt sind. In Verbindung mit einem Live Betriebssystem von CD gestartet verbleiben so keine nachweisbaren Spuren auf dem Computer, aus denen sich forensisch auswertbare Informationen ableiten ließen sobald der Rechner heruntergefahren wird. Unserer Meinung nach gibt es keine Beschränkung dafür wie viel Information so verborgen werden kann, zumal zum Missbrauch Mechanismen verwendet werden die jenen gleichen die von der Dropbox-Software selbst eingesetzt werden.

4.2 Angriffsvektoren

Ist dem Angreifer die Host-ID bekannt kann er beliebige Dateien hochladen und mit dem Account eines Opfers verlinken. Anstatt durch eine zweite HTTPS-Anfrage eine Verknüpfung mit dem eigenen Account anzufordern erfolgt diese mit einem willkürlich gewählten Account. In Kombination mit einer Schwachstelle in der Vorschaufunktion diverser Betriebssysteme ergibt sich so eine sehr effektive Angriffsmethode. Ein Angreifer könnte eine 0-day Schwachstelle dahingehend für seine Zwecke missbrauchen, als er eine manipulierte Datei in den Dropbox-

Ordner des Opfers einfügt und abwartet bis der Benutzer das Verzeichnis öffnet und über die Voransichtsfunktion Code ausgeführt wird. Über gezieltes Social Engineering könnte man ein Opfer ebenfalls zum Ausführen einer Datei mit vielversprechendem Namen bewegen. In Besitz der Host-ID zu gelangen gestaltet sich herausfordernder, zumal Zugang zum Dateisystem erforderlich ist. Ein Großangriff über diese Methode ist trotz allem recht unwahrscheinlich, denn jemand der in der Lage ist, in Besitz der Host-ID zu gelangen ist meistens bereits in der Lage das System zu übernehmen. Auch als „Covert Channel“ [16] oder um Daten aus einem Unternehmensnetzwerk zu schmuggeln ließen sich die hier beschriebenen Angriffe verwenden.

5 Auswertungen

Der folgende Abschnitt demonstriert einige der vorgestellten Angriffsszenarien. Wir überprüfen zum einen ob Dropbox dazu verwendet wird, gängige Dateien des Filesharing-Netzwerks *thepiratbay.org* zu hinterlegen, und wie lange Dateien im oben definierten *Online Slack Space* gespeichert werden können.

5.1 Auf Dropbox gespeicherte Daten

Mithilfe des Hash Manipulation-Angriffs sowie des Direkt Download Angriffs lässt sich leicht überprüfen, ob sich eine Datei bei bekanntem Hashwert bereits auf den Dropbox-Servern befindet. Anhand dieser Methoden haben wir getestet ob Dropbox zur Speicherung von Filesharing-Dateien verwendet wird, zumal einige Filesharing-Protokolle wie BitTorrent grundlegend auf Hashfunktionen zur Dateiidentifikation basieren. Dazu haben wir mit Stand Mitte September 2010 die Top-100-Torrents von thepiratebay.org heruntergeladen [7]. Aus urheberrechtlichen Gründen haben wir nur jene Dateien innerhalb der *.torrents* heruntergeladen, die nicht urheberrechtlich geschützt sind, aber trotzdem als Beweis fungieren, dass Dropbox als Speicherort für solche Inhalte verwendet wird. Unsere BitTorrent Software wurde auch dahingehend modifiziert, damit keine Daten zu anderen Nutzern geschickt werden [27]. Weiters fordert der von uns modifizierte Client jeweils nur das erste 4MB-Chunk an, da diese Information bereits ausreichend ist, um festzumachen, ob die jeweilige Datei bei Dropbox vorhanden ist.

Die in den *.torrent* enthaltenen Dateien können wie folgt klassifiziert werden:

- urheberrechtlich geschützte Inhalte wie Filme, Musikdateien oder Folgen beliebter Serien;
- „Identifizierende Dateien“, die zwar direkt an urheberrechtlich geschützte Dateien geknüpft sind wie z.B. Sample-Dateien, Screenshots oder Prüfsummendateien, ihrerseits aber nicht dem Urheberrecht unterliegen;

- Statische Dateien, zum einen die *.torrents* Datei selbst oder auch Dateien die Links zu Webseiten der Gruppe die sich für die *.torrent* Datei verantwortlich zeigt, enthalten

Die identifizierenden Dateien wiesen folgende Erweiterungen und Inhalte auf:

- *.nfo*: Informationen zum Ersteller des *.torrents*, Dateilisten, Installationshinweise oder detaillierte Informationen oder Bewertungen zu Filmen.
- *.srt*: beinhalten Untertitel zu Videodateien
- *.sfv*: beinhalten CRC32-Prüfsummen für jede Datei innerhalb der .torrent
- *.jpg*: beinhalten Screenshots von Filmen oder Album Covers
- *.torrent*: die BitTorrent-Datei an sich umfasst die Hashwerte aller Dateien, die Chunks sowie die für den Client nötigen Tracker-Informationen.

Von den Top-100 BitTorrent-Archiven enthielten 98 identifizierende Dateien, die zwei abweichenden *.torrents* entfernten wir aus dem Testset. Um herauszufinden, welche Zeitspanne in etwa zwischen Veröffentlichung eines BitTorrents und Hinterlegung auf Dropbox liegt, verglichen wir 24 Stunden später die aktuelle Top-100-Liste mit der bereits vorliegenden. 9 neue BitTorrents, hauptsächlich Folgen beliebter Serien, waren in der Zwischenzeit hinzugefügt worden. Wir erzeugten für jede *.torrent*-Datei und jede ihrer identifizierenden Datei SHA-256-Prüfsummen und überprüften, ob diese auf Dropbox zu finden sind. In Summe kamen wir so auf *368 Hashwerte*. In der Folge verwendeten wir den direkten Download Angriff mittels HTTPS um zu überprüfen ob die Dateien bei Dropbox gespeichert sind. 356 Dateien von insgesamt 368 waren abrufbar, die 12 verbleibenden waren demzufolge noch nie von einem Anwender bei Dropbox abgespeichert. Bei genauerer Betrachtung ergab sich aber, dass diese Fehler vereinzelt waren und die relevanten Inhalte auf Dropbox gespeichert waren. Das bedeutet dass für fast *100% der getesteten Dateien* auf Dropbox gespeichert werden, und es möglich gewesen wäre die Dateiinhalte über Dropbox herunterzuladen.

In weiterer Folge analysierten wir die Lebensdauer dieser *.torrents* und auch, wie schnell Dropbox-Nutzer diese und die dementsprechenden Inhalte downloaden und ihrerseits uploaden. Die meisten der *.torrent*-Dateien waren dabei sehr aktuell. Mehr als 20% der Top-100 *.torrent*-Dateien waren weniger als 24 Stunden auf piratebay.org, ehe wir über Dropbox darauf zugreifen konnten.

5.2 Online Slack Space Evaluation

Um zu überprüfen, ob man Dropbox dazu verwenden könnte, Dateien zu verbergen indem man nach dem Upload eine Verlinkung mit einem Useraccount unterbindet, haben wir ein Set von 30

Dateien mit zufälligem Inhalt generiert und diese über die HTTPS-Request-Methode hochgeladen. Um zu prüfen ob alte Daten vom Server entfernt werden, luden wir zusätzlich 55 mit Zufall als Inhalt über einen regulären Account auf Dropbox und löschten sie umgehend. Von den 55 Dateien befanden sich 30 in einer „Shared Folder“ und 25 in einem nicht gemeinsam verwendeten Ordner. Ferner untersuchten wir, ob eine Art „Garbage Collection“ existiert, die die Daten nach einer gewissen Zeitspanne entfernt. Wir luden die Dateien im 24-Stundentakt mittels dem HTTPS Direktdownload herunter und überprüften die Beständigkeit durch die Berechnung multipler Hashwerte.

Bis Ende April 2011, als Dropbox begonnen hatte, der HTTPS-Download-Attacke aktiv entgegenzuwirken, waren die 55 Dateien zu *100% durchgehend verfügbar.* Die Dateien waren auch mehr als sechs Monate nach dem Upload ausnahmslos vorhanden. Die über das HTTPS Interface hochgeladenen Dateien waren mehr als 4 Wochen verfügbar. Kurz vor einer Änderung von Dropbox um die HTTPS-Download-Attacke zu verhindern, sank die Verfügbarkeit auf 50%.

5.3 Diskussion der Ergebnisse

Wir waren überrascht, dass im Zusammenhang mit den jeweiligen *.torrent*-Dateien entweder der *.torrent*, der Inhalt oder beide über Dropbox abrufbar waren. Überraschend besonders deshalb, wenn man bedenkt das die *.torrent*-Dateien nur einige Stunden vor unserem Test erstellt wurden. 97% (356 von 368) Erfolgsrate weisen darauf hin, dass Dropbox in großem Maße zur Speicherung von Dateien aus Filesharing-Networks verwendet wird. Interessant ist auch anzumerken, dass der Inhalt mancher *.torrent*-Dateien bei weitem mehr Speicherplatz belegt als ein kostenloser Dropbox-Account umfasst (2 GB zum Zeitpunkt der Abhandlung). 11 der 107 getesteten *.torrents* verbrauchten mehr als 2 GB (mit 7,2 GB als Spitzenwert), da es sich um DVD-Images handelte. Daraus lässt sich schlussfolgern das die Person bzw. die Personen die diese Dateien auf Dropbox speichern einen Dropbox Pro Account (gegen eine monatliche Gebühr) oder durch das Anwerben von Freunden über das Dropbox-Bonusprogramm zusätzlichen Speicherplatz erworben hat. Aus unseren Untersuchungen können wir schlussendlich nur das Vorhandensein dieser Dateien ableiten, nicht aber quantifizierend feststellen, in welchem Ausmaß Dropbox unter den Benutzern zu Filesharing-Zwecken verwendet wird. Unsere Ergebnisse spiegeln nur wider, dass zumindest ein BitTorrent-User seine Downloads auf Dropbox abgelegt hat.

Unsere Untersuchungen zum Online Slack Space zeigen, dass es relativ einfach ist Daten versteckt auf Dropbox zu lagern, ohne strafrechtliche Folgen fürchten zu müssen. Außerdem zeigt es sich als recht simpel ohne zu zahlen an eigentlich kostenpflichtige Zusatzleistungen wie unlimitierte Dateiwiederherstellung oder erweiterte Dateiversionierung zu gelangen. Die Tatsache, dass man durch die Unterbindung des Verlinkens von Datei und Account unlimitierten Speicherplatz in Anspruch nehmen kann, resultiert in weiterer Folge aber auch in Erschwernissen hinsichtlich

diesbezüglicher forensischer Untersuchungen. In einem erweiterten Szenario könnten Ermittler sich sogar mit einem Computer ohne Festplatte konfrontiert sehen, der von einem Read-Only-Medium wie einer Linux Live-CD bootet und alle Daten im Online Slack Space ablegt. Ein solcher Computer würde keine brauchbaren Spuren oder lokale Beweise erzeugen [15]. Eine Problemstellung, die für die Computerforensik zukünftig sicher an Relevanz gewinnen wird, da es dem „Privatmodus“ moderner Browser gleicht, der keine Informationen lokal speichert [8].

6 Gegenmaßnahmen

Unsere Angriffe sind nicht nur in Bezug auf Dropbox anwendbar, sondern gefährden jedes Cloud Storage Service bei dem eine serverseitige Methode verwendet wird, um Übertragung und Speicherung von Dateiduplikaten vorzubeugen. Die derzeitigen Implementierungen basieren auf einfacher Prüfsummenbildung, doch kann man nicht von einer vollkommenen Vertrauenswürdigkeit der Client-Software in Bezug auf die korrekte Berechnung des Hashwertes ausgehen. Eine verlässlichere Überprüfung ob der Anwender wirklich im Besitz der Datei ist, sollte für jeden dieser Services implementiert werden. Es hat sich gezeigt, dass ein vollkommen neuer Aspekt aufzugreifen ist, denn bislang wurde in der Diskussion um die Vertrauenswürdigkeit dieser Dienste kaum auf die Gewichtigkeit des Clients als Sicherheitsschwachstelle eingegangen. Um sicherzustellen, dass sich der Client im Besitz einer Datei befindet ist ein verstärktes Protokoll nötig, egal ob nun auf Kryptographie basierend, auf statistischen Methoden, oder auf beidem.

Dies lässt sich über einen der jüngsten „Provable Data Possession“-Algorithmen wie in [11] verwendet umsetzen, bei denen der Cloud Storage Operator bestimmt, welche Anfragen der Client beantworten muss, ehe ihm Zugang zur Datei am Server gewährt wird. So lässt sich eine erneute Übertragung umgehen, die sowohl für den Nutzer als auch den Anbieter mit Kosten verbunden ist. Aktuelle Publikationen empfehlen unterschiedliche Ansätze mit unterschiedlichen Kosten [10, 12, 20]. Darüber hinaus sollte jeder Service seine Kommunikations- und Datentransferdienste über SSL abwickeln, was, wie wir feststellen konnten nicht immer der Fall ist.

Mehrere Schritte sind nötig um Dropbox abzusichern. Zu allererst muss ein Protokoll umgesetzt werden welches verhindert, dass der Hashwert einer Datei ausreicht, um diese abzurufen. Längerfristig sollte jeder Cloud Storage Operator ein solches Protokoll einsetzen, wenn der Client nicht als Teil der vertrauenswürdigen Umgebung angesehen werden kann. Wir raten zur Implementierung eines einfachen Challenge-Response-Mechanismus. Im Prinzip wird eine Zwischenschritt zu den bestehenden Protokollen eingefügt, während dem überprüft wird ob bei Übereinstimmung der Hashwerte der Client- und Serverdateien auch eine Übereinstimmung zufällig gewählter Dateibruchstücke vorliegt.

Das Hochladen von Chunks ohne Verknüpfung mit der Dropbox eines Anwenders sollte unterbunden werden, um einerseits unlimitierte Speicherplatzkapazität von bösartigen Anwendern entgegenzuwirken, und andererseits Online Slack Space zu verhindern. In manchen Fällen ist es immer noch kostengünstiger, zusätzliche Speicherkapazität anzufügen, als eine verlässliche Metrik zu entwickeln, welche Daten nun eigentlich zu löschen sind – will man jedoch den Missbrauch historischer Daten und von Online Slack Space verhindern, wird es dennoch unumgänglich, alle Chunks zu löschen, die nicht mit einer speziellen Datei in Verwendung verknüpft sind. Um die Sicherheitsvorkehrungen zusätzlich zu optimieren, können weitere behavioristische Aspekte einfließen. Zum Beispiel die Kontrolle der Host-ID-Aktivität: sobald ein Anwender seinen Computer hochfährt und über die Dropbox-Anbindung überprüft wird, können Transaktionen mit dieser Host-ID zugelassen werden. Im Anschluss sollte es nur mehr über diese IP-Adresse gestattet sein, Daten von der Dropbox dieser Host-ID herunterzuladen. Sollte sich die IP des Anwenders aufgrund der Verwendung eines VPN oder eines Standortwechsels ändern, muss die Verbindung zu Dropbox ohnehin neu aufgebaut werden und in diesem Zuge könnte die Zuordnung der Host-ID an die neuen IP erfolgen. Die Host-ID sollte, wenn zu Authentifizierungszwecken verwendet, wie ein Cookie eingesetzt werden: von dynamischer Natur und veränderlich. Doch vor allem muss von Dropbox verfolgt werden, welche Dateien sich in welcher Dropbox befinden. Fordert ein Anwender einen Chunk an, der sich nicht in seiner Dropbox befindet ist das für Dropbox leicht feststellbar.

Wir können kaum Angaben dazu machen, inwieweit unsere Verbesserungen, Auswirkungen auf die Geschwindigkeit oder Kosten zeigen, doch sind wir der Meinung, dass die meisten unserer Vorschläge über einfache Datenbankabfragen effizient zu implementieren wären. Verschiedene Datenbesitz-Algorithmen wurden bereits hinsichtlich ihres Overheads untersucht, so z.B. S-DPD und E-DPD von [11] welche durch O(1) in Ihrem Aufwand beschränkt sind.

7 Zusammenfassung

In diesem Artikel wurden einige Angriffe auf Cloud Storage Anbieter beschrieben, die dem Angreifer ermöglichen unter bestimmten Umständen Dateien unberechtigterweise herunterzuladen. Wir demonstrierten deren Anwendbarkeit anhand des Online Storage Anbieters Dropbox und konnten zeigen, dass Dropbox massiv dazu verwendet wird, Daten von *thepiratebay.org*, einer beliebten BitTorrent-Seite, abzuspeichern. Darüber hinaus definierten wir den Begriff *Online Slack Space* und konnten mittels unserer Untersuchungen zeigen, dass auf diese Art effektiv Daten im Internet versteckt werden können.

Wir sind davon überzeugt, dass sich diese Sicherheitsmängel keinesfalls auf Dropbox beschränken, da das zugrundeliegende Kommunikationsprotokoll sehr wahrscheinlich auch von anderen Cloud Storage Anbietern eingesetzt wird, um Bandbreite und Speicherkapazität einzusparen.

Die besprochenen Gegenmaßnahmen, allen voran die serverseitige Datenbesitzüberprüfung, sollten von allen Cloud Storage Anbietern umgesetzt werden.

Disclaimer

Die Details dieser Arbeit werden im August 2011 auch auf der USENIX Security Konferenz[2] in San Francisco vorgestellt.

Referenzen

[1] Amazon.com, Amazon Web Services (AWS). http://aws.amazon.com.

[2] At Dropbox, Over 100 Billion Files Served–And Counting, retrieved May 23rd, 2011. Online at http://gigaom.com/2011/05/23/at-dropbox-over-100-billion-files-served-and-counting/.

[3] Dropbox Users Save 1 Million Files Every 5 Minutes, retrieved May 24rd, 2011. Online at http://mashable.com/2011/05/23/dropbox-stats/.

[4] Grab the pitchforks!... again, retrieved April 19th, 2011. Online at http://benlog.com/articles/2011/04/19/grab-the-pitchforks-again/.

[5] How Dropbox sacrifices user privacy for cost savings, retrieved April 12th, 2011. Online at http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html.

[6] NCrypto Homepage, retrieved June 1st, 2011. Online at http://ncrypto.sourceforge.net/.

[7] Piratebay top 100. Online at http://thepiratebay.org/top/all.

[8] AGGARWAL, G., BURSZTEIN, E., JACKSON, C., BONEH, D. An analysis of private browsing modes in modern browsers. In Proceedings of the 19th USENIX conference on Security (2010), USENIX Security'10.

[9] ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A., STOICA, I., AND ZAHARIA, M. A view of cloud computing. Communications of the ACM 53, 4 (2010), 50–58.

[10] ATENIESE, G., BURNS, R., CURTMOLA, R., HERRING, J., KHAN, O., KISSNER, L., PETERSON, Z., AND SONG, D. Remote data checking using provable data possession. ACM Transactions on Information and System Security (TISSEC) 14, 1 (2011), 12.

[11] ATENIESE, G., BURNS, R., CURTMOLA, R., HERRING, J., KISSNER, L., PETERSON, Z., AND SONG, D. Provable data possession at untrusted stores. In Proceedings of the 14th ACM Conference on Computer and Communications Security (2007), CCS '07, ACM, pp. 598–609.

[12] ATENIESE, G., DI PIETRO, R., MANCINI, L., AND TSUDIK, G. Scalable and Efficient Provable Data Possession. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (2008), ACM, pp. 1–10.

[13] BOWERS, K., JUELS, A., AND OPREA, A. HAIL: A high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM Conference on Computer and Communications Security (2009), ACM, pp. 187–198.

[14] BOWERS, K., JUELS, A., AND OPREA, A. Proofs of retrievability: Theory and implementation. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (2009), ACM, pp. 43–54.

[15] BREZINSKI, D., AND KILLALEA, T. Guidelines for Evidence Collection and Archiving (RFC 3227). Network Working Group, The Internet Engineering Task Force (2002).

[16] CABUK, S., BRODLEY, C. E., AND SHIELDS, C. Ip covert timing channels: design and detection. In Proceedings of the 11th ACM Conference on Computer and Communications Security (2004), CCS '04, pp. 178–187.

[2] http://www.usenix.org/events/sec11

[17] CHOW, R., GOLLE, P., JAKOBSSON, M., SHI, E., STADDON, J., MASUOKA, R., AND M OLINA, J. Controlling data in the Cloud: Outsourcing Computation without Outsourcing Control. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (2009), ACM, pp. 85–90.

[18] COX, M., ENGELSCHALL, R., HENSON, S., LAURIE, B., YOUNG, E., AND HUDSON, T. Openssl, 2001.

[19] EASTLAKE, D., AND HANSEN, T. US Secure Hash Algorithms (SHA and HMAC-SHA). Tech. rep., RFC 4634, July 2006.

[20] ERWAY, C., KUPC U, A., PAPAMANTHOU, C., AND TAMASSIA, R. Dynamic Provable Data Possession. In Proceedings of the 16th ACM Conference on Computer and Communications Security (2009), ACM, pp. 213–222.

[21] GARFINKEL, S., AND SHELAT, A. Remembrance of data passed: A study of disk sanitization practices. Security & Privacy, IEEE 1, 1 (2003), 17–27.

[22] GOLAND, Y., WHITEHEAD, E., FAIZI, A., CARTER, S., AND JENSEN, D. HTTP Extensions for Distributed Authoring-WEBDAV. Microsoft, UC Irvine, Netscape, Novell. Internet Proposed Standard Request for Comments (RFC) 2518 (1999).

[23] GROLIMUND, D., MEISSER, L., SCHMID, S., AND WATTEN-HOFER, R. Cryptree: A folder tree structure for cryptographic file systems. In Reliable Distributed Systems, 2006. SRDS'06. 25th IEEE Symposium on (2006), IEEE, pp. 189–198.

[24] HARNIK, D., PINKAS, B., AND SHULMAN-PELEG, A. Side channels in cloud services: Deduplication in cloud storage. Security & Privacy, IEEE 8, 6 (2010), 40–47.

[25] JUELS, A., AND KALISKI JR, B. PORs: Proofs of retrievability for large files. In Proceedings of the 14th ACM Conference on Computer and Communications Security (2007), ACM, pp. 584–597.

[26] KRISTOL, D. HTTP Cookies: Standards, privacy, and politics. ACM Transactions on Internet Technology (TOIT) 1, 2 (2001), 151–198.

[27] PIATEK, M., KOHNO, T., AND KRISHNAMURTHY, A. Challenges and directions for monitoring P2P file sharing networks - or: why my printer received a DMCA takedown notice. In Proceedings of the 3rd Conference on Hot Topics in Security (2008), USENIX Association, p. 12.

[28] POSTEL, J., AND REYNOLDS, J. RFC 959: File transfer protocol. Network Working Group (1985).

[29] SCHWARZ, T., AND MILLER, E. Store, forget, and check: Using algebraic signatures to check remotely administered storage. In Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on (2006), IEEE, p. 12.

[30] SUBASHINI, S., AND KAVITHA, V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications (2010).

[31] WANG, C., WANG, Q., REN, K., AND LOU, W. Ensuring data storage security in cloud computing. In Quality of Service, 2009. IWQoS. 17th International Workshop on (2009), Ieee, pp. 1–9.

[32] WANG, Q., WANG, C., LI, J., REN, K., AND LOU, W. Enabling public verifiability and data dynamics for storage security in Cloud Computing. Computer Security–ESORICS 2009 (2010), 355–370.

TRUST CENTER CONTROLLED CODE ACCESS SECURITY (TC³ AS)

Grischa Schmiedl, Kerstin Blumenstein

Aus Sicherheitsgründen ist der Zugriff auf lokale Ressourcen für Webanwendungen eingeschränkt. Vor allem mobile Websites [3] können die erweiterten Fähigkeiten mobiler Plattformen nicht nutzen. Das Konzept der Trust Center Controlled Code Access Security (TC³AS) soll einerseits die sichere Aufhebung von Beschränkungen von Web Applikationen gewährleisten und andererseits dem User eine verständliche und einfache Konfiguration der Sicherheitseinstellungen ermöglichen.

1 Einleitung

Nachdem der Mobilfunkmarkt in Bezug auf Neukundengewinnung mittlerweile als gesättigt gilt, wird das mobile Web als die Hoffnung der Mobilfunkindustrie gehandelt. Web Applikationen haben aus Sicherheitsgründen aber nur eingeschränkten Zugriff auf die Ressourcen sowie die Hardware des lokalen Systems (Sandbox-Prinzip). Die Notwendigkeit dieser Einschränkungen ergibt sich dadurch, dass Webapplikationen nicht am lokalen System installiert werden, sondern nur durch das Aufrufen einer Webseite „gestartet" werden und somit „fremder" und damit potentiell gefährlicher Code auf dem lokalen System ausgeführt wird.

Obwohl Aufweichungen dieses Sicherheitskonzeptes existieren[4], sind viele Applikationen mit Web Technologien derzeit nicht realisierbar. Dies betrifft sowohl Webanwendungen am gewöhnlichen PC als auch mobile Applikationen, bei denen z.B. der Standort[5], aber auch die in den Geräten verbaute Hardware (Kamera, Gyrometer etc.) oft einen entscheidenden Mehrwert für Applikationen bringt.

[3] Herkömmliche Webanwendungen können auf mobilen Geräten weitgehend problemlos angezeigt werden. Für eine optimale Bedienbarkeit sollten diese zumindest „mobile aware" ausgeführt werden. Eine Alternative ist eine die normale Website ergänzende „mobile optimized" Version für Smartphones, deren Presentation Layer auf die Besonderheiten der mobilen Geräte optimiert ist [2] und idealer Weise die technischen Fähigkeiten der Geräte nutzen sollte (Lage- und Positionssensorik, Kamera etc.).

[4] Aufweichungen des Prinzips existieren bereits im Bereich der RIA-Plugins, z.B. bei Adobe Flash (Zugriff auf Kamera, Mic) und bei Silverlight (Protected local Storage). Für Java Applets kann durch das Signieren des Codes der Zugriff auf das gesamte System gewährt werden. HTML5 bringt ebenfalls einen erweiterten aber dennoch nach wie vor beschränkten Zugriff auf lokale Ressourcen.

[5] Der Zugriff auf die Location-Daten (z.B. GPS-Position) ist per HTML5 möglich, die Methode der Zugriffsbeschränkung durch Nachfragen beim User für jede einzelne Applikation aber nicht zufriedenstellend.

Um diese Einschränkungen zu umgehen, bieten viele Hersteller von Webapplikationen[6] als Alternative gerätespezifische *Native Applications* für diverse Betriebssysteme im Mobilfunkbereich an, die diesen Beschränkungen nicht unterliegen. Der Download sowie die Installation dieser Anwendungen aus den bei mobilen Plattformen mittlerweilen gängigen *Application Stores*[7] des Betriebssystem-Anbieters wird dem User extrem einfach gemacht.

Native Applications haben vollen Zugriff auf das System. Ihre Inbetriebnahme ist aber kaum komplizierter als das Aufrufen einer Webseite – und die AnwenderInnen zeigen nur wenig Scheu, Programmen, deren Vertrauenswürdigkeit sie genau so wenig beurteilen können wie die von Web Applikationen, unlimitierten Zugriff auf ihr Gerät zu geben.

2 Hintergrund und Zielsetzung

In diesem Paper beschreiben wir das Konzept einer Methode, mit der Web Applikationen über ein normiertes Application Programming Interface (API) Zugriff auf alle Bereiche des Systems bekommen können. Die tatsächlichen Rechte einer Applikation werden durch ein userfreundliches Rechtemanagement-System festgelegt. Die Problematik der Konfiguration von Sicherheitsrichtlinien besteht aus Usabilitysicht darin, dass die Konfiguration der Sicherheitseinstellungen der BenutzerIn einerseits keine direkt nutzbaren Vorteile bringt (die Applikation funktioniert dadurch nicht „besser“) und andererseits viele BenutzerInnen mit der Aufgabe schon auf Grund mangelnden Verständnisses für die Gefahren überfordert sind. In [3] analysierten Braz und Robert diverse IT-Sicherheitssysteme und mussten sehr oft mangelhafte Usability diagnostizieren. Tatsächlich bricht bereits ein typischer Login-Dialog sechs der acht von Shneiderman vorgeschlagenen „goldenen Regeln“ des User Interface Design [15].

Das Ziel dieses Rechtemanagementsystems ist es, eine für die AnwenderIn rasche und sichere Konfigurationsmöglichkeit anzubieten, mit welcher der Zugriff von Applikationen auf das eigene Gerät gesteuert und überwacht werden kann. Die notwendigen Konfigurationsschritte für die AnwenderIn sollen minimiert werden, ohne die Möglichkeit zur detaillierten Steuerung zu verweigern. Damit soll das System eine Lösung zu dem bereits in [11] beschriebenen Problem bieten, dass AnwenderInnen auf Grund der hohen Komplexität bestehende Sicherheitssysteme nicht richtig konfigurieren können. Dieses Rechtemanagementsystem soll vor allem im Bereich von Webapplikationen zum Einsatz kommen. Es lässt sich aber im Prinzip auch auf Desktop Applikationen, die einem Codesicherheitssystem unterliegen (z.B. Java, .Net), anwenden.

[6] U.a. Google, Youtube, eBay sowie diverse Communityportale

[7] Application Stores existieren mittlerweile für alle modernen Smartphones z.B. für das iPhone (App Store), Android-Geräte (Market), Windows Phone 7 (Marketplace), BlackBerry (BlackBerry App World) und für Nokia (Ovi Store).

3 Anforderungen an das System

Folgende Anforderungen werden an das System gestellt:

- Das System soll für die BenutzerInnen einfach verständlich und einfach konfigurierbar sein. Es soll verhindert werden, dass die BenutzerIn für jede Applikation den Zugriff auf diverse Funktionen einzeln konfigurieren muss.
- Die Freigabe soll nicht für jede Applikation einzeln getroffen werden müssen. Sie ist mit einem Zertifikatssystem eines globalen oder lokalen (Intranet-Sicherheit) Trust Centers verbunden, das die Rechte vergibt.
- Die Rechte sollen für Gruppen gesetzt werden, in denen ähnliche Applikationen zusammengefasst sind. Die Gruppierung soll nicht durch die AnwenderIn selbst erfolgen müssen.
- BenutzerInnen sollen vor Start der Applikationen sehen, welchen Zweck ein Programm verfolgt und welche Zugriffe es benötigt. Das System soll nur genau diese Zugriffe ermöglichen. Es muss gewährleistet sein, dass ein Programm nur den genannten Zweck erfüllt.
- Die Bewertung der Vertrauenswürdigkeit eines Anbieters bzw. einer Applikation soll nicht der BenutzerIn allein überlassen werden. Eine zentrale Instanz (~Trust Center), die Applikationen hinsichtlich ihres Einsatzzwecks zertifiziert, soll die BenutzerIn dabei unterstützen.
- Das Trust Center unterstützt die BenutzerIn bei der Vergabe der notwendigen Rechte, zeigt Gefahrenpotentiale auf und kann nachträglich Applikationen Rechte wieder entziehen.
- Die Rechte, die einer Applikation oder Applikationsgruppe von der BenutzerIn zugestanden werden, können für zentral administrierte Geräte (z.B. Company-Smartphones) eingeschränkt werden (Company-Policy merged with User Policy).
- Der Zugriff auf die geschützten Funktionen erfolgt über ein genormtes Application Programming Interface (API). Web Applikationen müssen anmelden, welche Rechte sie (wofür) benötigen, bevor Sie mit Hilfe dieses API Zugriff auf ein lokales System bekommen. Die BenutzerIn kann diese Berechtigung für diese Session oder generell für diese Applikation bzw. Applikationsgruppe erteilen oder verweigern. Das System soll den User bei einer Automatisierung dieser Rechtevergabe unterstützen.
- Wird eine Berechtigung einmal dauerhaft erteilt, kann der User diese jederzeit einsehen, widerrufen oder ändern. Außerdem wird die Verwendung der Schnittstelle der AnwenderIn generell angezeigt, auch wenn nicht nachgefragt wird.

- Die Zugriffe auf das API durch eine Applikation werden vom API geloggt. Ein Missbrauch kann an das Trust Center berichtet werden, welches das Zertifikat entziehen kann.
- Die Einstellungen einer BenutzerIn können im Trust Center abgelegt und daher auch auf andere Geräte der NutzerIn mitgenommen werden.

4 Trust Center Controlled Code Access Security

Im Folgenden wird das Konzept eines Trust Center-gesteuerten Rechtemanagementsystems für Web Applikationen vorgestellt.

4.1 Bestehende Ansätze zur Codesicherheit

Es gibt diverse Ansätze, die Rechte einer Applikation einzuschränken. Im Bereich der Web Applikationen können die Sicherheitsrichtlinien im Browser entweder sehr grob (z.B. IE-Sicherheitsstufe) oder sehr (zu) detailliert vergeben werden. Die Rechte sind meist für alle Applikationen einer Sicherheitsklasse (Intranet, Internet, Local Zone etc.) identisch. Bestimmte Möglichkeiten können für eine Sicherheitsklasse meist nur komplett an- oder abgeschaltet werden (z.B. JavaScript deaktivieren). In anderen Systemen können manche Rechte (z.B. Zugriff auf das lokale System durch signierte Java-Applets) pro Applikation (identifiziert durch URL) oder pro Hersteller (identifiziert durch den in der Signatur festgelegten Hersteller) eingestellt werden.

Jeweils eigene Ansätze für Code Access Security existieren für Java / Java Applets, das .Net Framework, diverse Browser (Firefox, IE ...) getrennt sowie für diverse Browser Plug-Ins (Flash, Silverlight).

Die Konfiguration der Sicherheitsrichtlinien wird vom User selbst durchgeführt oder kann im Unternehmensbereich durch den Systemadministrator zentral vorgegeben werden. In vielen Fällen wird der User vom System zu einer sicherheitsrelevanten Entscheidung gezwungen, um eine Anwendung verwenden zu können. So muss bei den gängigen Implementationen von HTML5 (z.B. im Safari-Browser des iPhones) der Zugriff auf die Position vom User für jede einzelne Applikation freigegeben werden. EndbenutzerInnen sind mit der Konfiguration der Sicherheitsrichtlinien oft nicht nur überfordert, die Sicherheitsnachfragen werden meist auch als lästig empfunden.

4.2 Der Trust Center Ansatz

Der Begriff Trust Center wird im Bereich der IT-Security für das Schlüsselverwaltungszentrum einer PKI (Public Key Infrastructure) eingesetzt.

Zertifikate bzw. Signaturen einer PKI garantieren die Identität einer Person oder Organisation bzw. die Authentizität von Dokumenten, Webseiten, Programmen etc. [5]

Das Konzept der Trust Center Controlled Code Access Security geht über diese Aufgaben hinaus und basiert auf folgenden Ideen:

- Die Applikationen diverser Hersteller werden in vordefinierte Applikationsklassen eingeteilt. Für diese *Purpose Classes* sind die für den Zweck der Software benötigten Rechte allgemein gültig definiert. Die Zuteilung einer Applikation zu einer Purpose Class ergibt sich aus dem „Zweck" der Applikation.
- Die Purpose Classes für eine Applikation werden zentral zugewiesen. Dies muss nicht von der EndanwenderIn entschieden werden.
- Ein Trust Center im Trust Center Controlled Code Access Security-Konzept kann von unterschiedlichen Institutionen und Organisationen intern oder öffentlich betrieben werden.
- Das Trust Center bestätigt nicht nur die Identität des Herstellers und die Authentizität der Software, sondern legitimiert auch den Zugriff der Software auf das lokale System.

4.3 Funktionen des Trust Centers

Das Trust Center vereint zwei Funktionen. Einerseits stellt es die Identität eines Anbieters bzw. dessen Angebotes an Applikationen durch Zertifikate sicher. Andererseits realisiert es eine Art Gütesiegel für zertifizierte Anwendungen, das die Applikation einer bestimmten Purpose Class zuordnet und die Einhaltung der Kriterien dieser Purpose Class garantiert.

Die Zuordnung einer Applikation zu einer Purpose Class erfolgt immer durch den Anbieter der Applikation, der seine Anwendung bei einem Trust Center anmeldet. Die Anmeldung beinhaltet neben der URL der Anwendung und der Identifikation des Anbieters auch ein *Mission Statement* des Anbieters, in dem er den genauen Zweck der Applikation erklärt. Je nach Zertifikatsgüte kann die Evaluation der Zuordnung entweder durch das Trust Center durchgeführt und die Zugehörigkeit damit formal bestätigt werden oder die formale Überprüfung unterbleibt. In beiden Fällen ist die Zuordnung einer Applikation zusätzlich einer durch das Trust Center realisierten *Community-Based Evaluation* unterworfen.

Um sicherzustellen, dass eine Applikation nach Vergabe des Zertifikats nicht verändert wird, können herkömmliche kryptologische Verfahren (Code-Hashes, Code-Signing) angewendet werden. Damit kann allerdings der serverseitige Teil der Anwendung nicht überprüft werden.

Abbildung 1 zeigt die Kommunikation der Komponenten, bestehend aus dem *Extensible Device API* am Client, dem Applikationsanbieter und dem Trust Center.

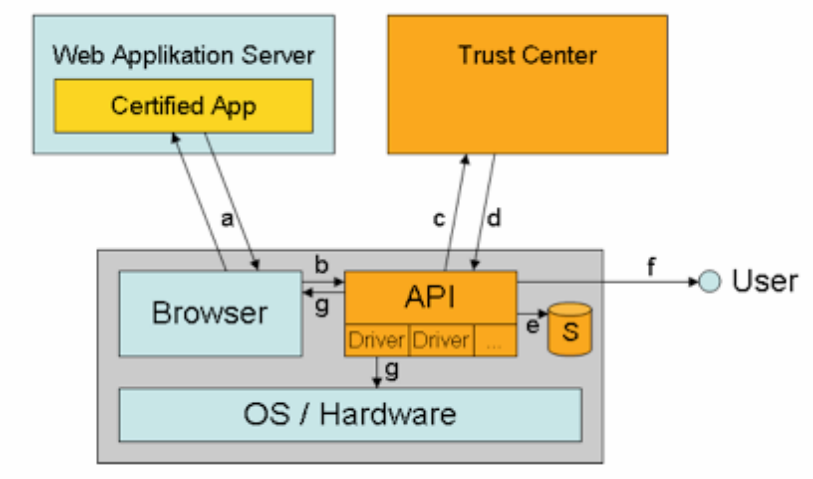


Abbildung 1 - Trust Center Architektur

Die Kommunikation erfolgt in folgender Weise:

- Die AnwenderIn navigiert auf die Seite des Anbieters einer Applikation, welche das Extensible Device API einsetzt.
- Um das API aufrufen zu können, muss sich die Applikation bei dem API mit Ihrer Zertifikatskennung anmelden.
- Das API evaluiert die Gültigkeit des Zertifikats beim Trust Center, das dieses Zertifikat ausgestellt hat. Das Trust Center muss im Browser als vertrauenswürdig eingestuft sein.
- Das Trust Center bestätigt die Authentizität des Zertifikats und übermittelt dem API:
    - Die URL der Anwendung, anhand der das API erkennen kann, ob die Anwendung vom richtigen Anwender stammt
    - Das Mission Statement des Anbieters zu der Anwendung; der User kann sich daher anhand der Beschreibung des Anbieters vorab über die Applikation informieren
    - Allfällige Userbewertungen aus der Community-Based Evaluation
    - Die Purpose Class für die diese Applikation angemeldet ist, sowie die Rechte, die sich aus der Purpose Class ergeben, wenn diese im API nicht vorhanden sein sollten
    - Die Art des Zertifikats (self-paced oder Trust Center evaluated)
- Das API überprüft auf Basis der lokalen Einstellungen, wie mit der Applikation weiter verfahren werden soll. Die Entscheidung basiert im Normalfall auf den Usereinstellungen in Bezug auf die Purpose Class und der Art des Zertifikats. Denkbar ist auch den Zertifikaten

eines bestimmten Trust Centers oder einem bestimmten Anbieter generell höheres Vertrauen entgegenzubringen. Die Möglichkeiten sind:

  - Zugriff ohne Nachfragen erlauben
  - Zugriff mit Nachfragen erlauben
  - Zugriff verweigern

- Im Falle von „Zugriff mit Nachfragen erlauben“ wird der AnwenderIn das Zertifikat mit sämtlichen Daten vor allem aber auch dem Mission Statement und allfällige Bewertungen aus der Community-Based Evaluation angezeigt. An dieser Stelle könnte die AnwenderIn Applikationen dieses Trust Centers, dieses Anbieters oder nur dieser Applikation für die Zukunft erweiterte Rechte einräumen, z.B. „Allen Applikationen der Purpose Class „POI“ ohne Nachfragen vertrauen, wenn sie vom Unternehmen XY stammen“.
- Der Applikation wird vom API ausschließlich auf die Ressourcen Zugriff gewährt, die der Purpose Class entsprechen.

4.4 Purpose Classes

Applikationen werden in *Purpose Classes* eingeteilt. Diese Einteilung richtet sich nach dem Zweck, den eine Applikation verfolgt und legt die für diesen Zweck benötigten Zugriffe auf Ressourcen des lokalen Systems fest. Der Zweck bezieht sich nicht nur darauf, welche Daten benötigt werden, sondern auch, wie bestimmte Daten verwendet werden.

So könnten Applikationen, welche die Location der AnwenderIn nur dafür verwenden, um dieser nahe gelegene *Points of Interest (POIs)*[8] anzuzeigen, in einer Purpose Class „POI“ zusammengefasst werden. Ein gänzlich anderer Anwendungszweck der Location (also der gleichen Ressource) ist aber, wenn die Location anderen BenutzerInnen weitergegeben wird (z.B. Buddydienste, Fleet Management).

Dieses Bespiel zeigt, dass die Zusammenstellung der Purpose Classes nicht nur als Kombination verschiedener Zugriffsrechte gesehen werden darf. Es wirft gleichzeitig die Frage auf, wie gewährleistet werden kann, dass Applikationen die erworbenen Daten nur klassenkonform verwenden.

Statt der Konfiguration der Rechte zum Zugriff auf einzelne lokale Ressourcen soll die Vergabe der Rechte durch die BenutzerIn auf Basis der *Purpose Classes* erfolgen. In einer Purpose Class ist

[8] Bsp. für POIs sind Apotheken, Geldautomaten, Restaurants,... in der Umgebung des Anwenders. So die Anwendung nicht auch einen „Routenfinder“ mit genauen Anweisungen, wie man zu dem POI kommt, enthält, ist die per GPS realisierbare metergenaue Position nicht notwendig. Die den Applikationen der Klasse POI zur Verfügung gestellte Position könnte also absichtliche – vom Anwender konfigurierbare – Abweichungen enthalten.

genau festgelegt, welche Rechte benötigt werden. Gibt ein User eine Purpose Class frei, so können alle Applikationen, die zu dieser Klasse gehören, auf alle Features zugreifen, die dieser Klasse angehören. Beim ersten Aufruf der Applikation meldet das System dem User, zu welcher Klasse die Applikation gehört und fragt nach, ob der Zugriff auf die Klassenfeatures dieser Applikation gewährt werden soll.

4.5 Definition der Purpose Classes

Eine große Herausforderung ist mit Sicherheit die Erstellung sinnvoller Purpose Classes. Die Anzahl an Purpose Classes muss gering gehalten werden, um der EndanwenderIn nicht erneut Probleme bei der Konfiguration zu bereiten. Die Vereinfachung der Konfiguration ist eines der Ziele zur Schaffung der Purpose Classes. Es ist aber nicht anzunehmen, dass jede nur denkbare Anwendung perfekt in eine der Purpose Classes passen wird. Die Klassen haben einen gewissen Spielraum und beschränken sich darauf, die Zugriffe auf mehrere Ressourcen sowie die datenschutzrelevante Verwendung einzuschränken.

Als Ausweg für nicht einteilbare Applikationen bleiben folgende Varianten:

- Individual-Applikation ohne Purpose Class: Solche Applikationen müssen im Vorhinein bekannt geben, welche Systemzugriffe sie benötigen. Im Mission Statement wird der Verwendungszweck der Daten deklariert. Der User entscheidet anhand der einzelnen benötigten Rechte, ob er die Applikation zulässt. Dieses für die AnwenderIn umständliche „Fall Back Szenario“ ist derzeit bei jenen Systemen im Einsatz, die eine feine Konfiguration der Sicherheit eines Systems unterstützen.
- Vollzugriff für die Applikation: Diese scheinbar undenkbare Variante ist die Realität bei den Native Applications, die als Alternative zu Web Applikationen derzeit angeboten werden.

4.6 Bedeutung des Mission Statements

Das Mission Statement ist eine vom Hersteller der Software verfasste Erklärung, welchen Zweck die Anwendung erfüllt und was mit den übertragenen Daten passiert (z.B. eventuelle Speicherung oder Weitergabe von Location-Daten). Eine technische Überprüfung, ob der Anbieter sein Mission Statement einhält, ist durch die hier vorgestellte Methode nicht möglich. Das Mission Statement ist daher eher als Vertrag zu sehen, den der Anbieter allen AnwenderInnen anbietet. Die Nichteinhaltung des Mission Statements ist demnach als Vertragsbruch zu bewerten. Das Mission Statement ist als Verfeinerung der Regeln, die für eine Purpose Class gelten, zu sehen. Es darf den Regeln der Purpose Class nicht widersprechen.

4.7 Promoter Zertifikate

Im bisherigen Konzept wird das Zertifikat immer von der Zertifikatsstelle allein ausgestellt. Dieses Zertifikat ist dann prinzipiell weltweit gültig. Möchte eine Organisation bzw. Unternehmen für die eigenen Mitglieder / MitarbeiterInnen nur bestimmte Applikationen freigeben (d.h. diese Applikationen sollen auf die für sie relevanten Funktionen der Schnittstelle zugreifen können), kann diese Organisation eine eigene Zertifikatsstelle implementieren – analog zu einem Zertifikatszentrum in einer unternehmensinternen PKI.

Alternativ kann sie aber auch als Promoter dieser Applikationen bei einer öffentlichen Zertifikatsstelle auftreten. Als Promoter übernimmt sie die Aufgabe eine Applikation und deren Hersteller zu überprüfen. Ein Zertifikat einer öffentlichen Zertifikatsstelle kann einen oder mehrere Promotoren haben. Am Gerät der EndanwenderIn kann eingestellt werden, Zertifikaten immer zu vertrauen, die einen bestimmten Promoter aufweisen. Unternehmen können diese Vertrauensstellung auf den Geräten ihrer MitarbeiterInnen einmal einrichten und danach beliebig viele Zertifikate (und damit Applikationen) promoten.

Die Methode eignet sich besonders für Unternehmen, die Applikationen von Application Service Providern (ASP) zukaufen, diese also nicht selbst betreiben. Hier hält der Provider die Lizenz für die erforderlichen Systeme und Software [16].

Die Authentizität eines Promoters in einem Zertifikat wird durch herkömmliche digitale Zertifikate gewährleistet.

5 Extensible Device API

Derzeit zeichnet sich nur im Bereich der Geolocation eine Standardisierung für APIs ab, die im Browser angesprochen werden können. Für andere Ressourcen gibt es noch keine Standards.

Da die Code Access Security nicht nur bestehende Ressourcen sondern auch erst zukünftig eventuell zur Verfügung stehende Ressourcen (z.B. RFID-Reader im Handy) behandeln soll, muss es zumindest den Ansatz einer erweiterbaren Schnittstelle für diverse Ressourcen geben.

5.1 Bestehende Ansätze

Es gibt bereits mehrere Ansätze zur Erweiterung der Fähigkeiten einer Browserapplikation. Dazu zählen die erweiterten Möglichkeiten von Flash (Zugriff auf Kamera, Mikrophon) und Silverlight (local storage, local database).

Bemerkbar ist auch der Trend zu APIs, auf die im Browser über JavaScript zugegriffen werden können:

- Das W3C hat im September 2010 die Candidate Recommendation der „Geolocation API Specification“ freigegeben. Die *privacy considerations* besagt, dass der User sein Einverständnis zur Nutzung der Schnittstelle geben muss. Diese Einwilligung muss für die AnwenderInnen widerrufbar sein. [10]
- Das Google Gears Framework realisiert u.a. Offline Access, Local Storage und Geolocation. Die Rechtevergabe im Framework basiert auf Freigaben auf Einzelapplikationsebene bei jedem Zugriff. Aktuell weist Google die Gears Ressourcen als überholt (deprecated) aus [8]. Grund ist das Ziel, die Ressourcen in den HTML5-Standard einzuarbeiten [9]. Ansätze dafür sind das eben beschriebene Geolocation API sowie FileAPI, Web Storage und Offline Web Application [6, 10, 14, 17].
- Fire Eagle ist ein serverbasierter Ansatz, bei dem die Location von einer Anwendung am Gerät des Users zum Fire Eagle Service geschickt wird und anschließend von Web Applikationen abgefragt werden kann. Die Information wird immer über das Fire Eagle Service verwaltet. Der Zugriff des Service erfolgt über http(s). [7]
- Geode: Die Firefox Extention für Geolocation implementiert das W3C Geolocation API. Seit Version 3.1 von Firefox ist das API ein fester Bestandteil des Browsers [13]. Die Schnittstelle wird ebenfalls in der mobilen Version des Firefox unterstützt.
- Während sich im Bereich der Geolocation mit der Candidate Recommendation der Geolocation API Specification in [10] eine Standardisierung abzeichnet, ist im Bereich anderer Erweiterungen (local file access, Kamera/Mic-Support) bisher kein Standard zu erkennen.

Im Bereich der Sicherheit sehen zwar alle Ansätze vor, die erweiterten Fähigkeiten nur dann einer Web Applikation zur Verfügung zu stellen, wenn dies durch den User legitimiert wird, die damit verbundene Komplexität für den User wird aber kaum diskutiert.

5.2 Extensible Device API für Web Applikationen

Bei der Definition einer Schnittstelle, die auf möglichst vielen Endgeräten zum Einsatz kommen soll, ist es wichtig, bestehende Implementationen und Spezifikationen nicht zu ignorieren.

Das API soll daher einer modularen Architektur entsprechen, bestehend aus dem generischen Interface für die darauf basierenden Applikationen und hersteller- bzw. gerätespezifischen Treibern.

Folgende API-Teile sind von den spezifischen Treibern und Implementationen unabhängig und daher immer vorhanden:

- Authorization-Interface: Funktionen, die zur Anmeldung der Applikation an das API verwendet werden.
- Supported Device Interface: ermöglicht der Applikation herauszufinden, welche der für diese Applikation prinzipiell autorisierten Devices auf dem konkreten Gerät auch tatsächlich verfügbar sind.

Es ist möglich, über das Extensible Device API auch bestehende APIs einzubinden (z.B. die HTML5-Extentions für Geolocation). Der Zugriff auf die Ressourcen wird dann nicht mehr auf die vorgesehene Weise kontrolliert (z.B. durch Nachfragen beim User), sondern dem Extensible Device API überlassen. Sollen die bestehenden APIs nicht verändert werden, kann das Extensible Device API auch als Ergänzung zu bestehenden Systemen eingesetzt werden. Wird das bestehende API auf gewohntem Weg (nicht über das Extensible Device API) aufgerufen, so kommt deren normales Sicherheitssystem zum Einsatz. Die Kompatibilität zu bestehenden Applikationen bleibt also erhalten. Erfolgt der Zugriff aber über das Extensible Device API, so soll keine weitere Überprüfung durch das Sicherheitssystem der bestehenden Schnittstelle erfolgen müssen.

6 Einsatzszenarien

Im folgenden Abschnitt werden ausgewählte Einsatzszenarien vorgestellt, in denen die Trust Center Controlled Code Access Security zum Einsatz kommen könnte.

6.1 Softwarehersteller für Web Applikationen

Der Softwarehersteller möchte Websites herstellen, die speziell den Mobilmarkt ansprechen und mobil einen Mehrwert gegenüber der Nutzung am PC versprechen. Für die volle Funktionalität wird direkter Zugriff auf das Telefon benötigt.

Die Erstellung von Native Applications für die diversen Plattformen ist keine Alternative, da der Aufwand durch die vielfältigen und völlig verschiedenen Development-Umgebungen am Handymarkt zu groß wäre und die MitarbeiterInnen des Herstellers nicht die benötigten Skills (C++, C#, Java, Objective-C usw.) aufweisen. Die Anwendung ist in erster Linie eine typische Webanwendung (Informationsanwendung), die mobile Szenarien optimal unterstützen soll, aber auch als Web Anwendung genutzt werden kann.

Um dies zu ermöglichen, verwendet der Anbieter die TC^{3}AS-Infrastruktur und bietet die erweiterten Funktionen an. BenutzerInnen, die das API aus der TC^{3}AS-Infrastruktur nicht installiert haben (oder dem Anbieter nicht vertrauen), können nur die erweiterten Funktionen nicht verwenden, der Rest der Applikation ist benutzbar.

6.2 Application Service Provider (ASP) / Unternehmenskunde

Ein ASP möchte branchenspezifische Lösungen für AußendienstmitarbeiterInnen von Unternehmen herstellen. Die MitarbeiterInnen / Unternehmen haben unterschiedliche Endgeräte. Die Unternehmen möchten die Lösung vom ASP betreiben lassen. Aus Sicherheitsgründen soll die Funktionalität der Software eingeschränkt sein. Außerdem benötigt die Applikation erweiterten Zugriff auf die Hardware. Eine normale Web Anwendung ist daher nicht ausreichend.

Ein Beispiel dafür wäre eine Versicherung, die ihre AußendienstmitarbeiterInnen zur Schadensaufnahme mit mobilen Geräten ausstattet. Fotos des Schadenfalls, werden gemeinsam mit den erhobenen Daten und dem Ort der Schadensaufnahme automatisch an den Versicherungsrechner geschickt. Die Software benötigt also folgende Zugriffe auf die eingebaute Kamera des mobilen Gerätes, die Position (Location) und eventuell auf den lokalen Speicher (Zwischenspeicher bei schlechter Verbindung).

Der ASP verwendet die TC^{3}AS-Infrastruktur und erwirbt ein Zertifikat bei einer beliebigen Zertifikatsstelle. Das Versicherungsunternehmen testet die Software und tritt selbst als Promoter der Software auf. Die mobilen Geräte der MitarbeiterInnen werden so konfiguriert, dass sie allen Lösungen dieses Promoters (also der eigenen Firma) vertrauen. Damit sind alle Lösungen verschiedener Hersteller (oder auch des Unternehmens selbst) für die MitarbeiterInnen freigeschalten, die von dem Unternehmen promotet werden.

Das Einspielen von Updates erfolgt nur auf der Serverseite des Anbieters. Das Unternehmen kann jederzeit die Promotion für eine Software beenden. Damit kann sie von den MitarbeiterInnen nicht mehr eingesetzt werden. Die Software hat nur Zugriff auf die im Zertifikat angegebenen Funktionen. Sie ist also im Vergleich zu Native Applications eingeschränkter und damit sicherer.

6.3 Promoter: Interessensvertretung

Als Erweiterung des beschriebenen Szenarios kann auch eine Interessenvertretung (z.B. Verein, Fachverband, Verlag) als Promoter von Softwarelösungen auftreten. So könnte z.B. ein branchenspezifischer Fachverband Software für diese Branche (z.B. Ärztekammer, Fachverbände) oder ein Verlag, der Software testet und bewertet, diese Lösungen promoten (z.B. Ich vertraue jeder von meiner Interessensvertretung als gut befundene Site automatisch).

Denkbar wäre auch ein Geschäftsmodell, bei dem ein Promoter (z.B. ein Branchenspezialist) für seine Dienstleistung des Testens und Promotens vom Kunden bezahlt wird. Der Promoter tritt damit (rechtlich) als Vermittler zwischen den Anbietern und den Kunden auf, ähnlich eines Versicherungsmaklers, der die Angebote mehrerer Versicherungen prüft und den Kunden die beste Variante vermittelt.

6.4 Unternehmen mit eigener Infrastruktur

Ein Unternehmen betreibt seine eigenen Webanwendungen für seine MitarbeiterInnen. Die Anwendungen sollen auf die lokalen Ressourcen des mobilen Gerätes Zugriff haben. Jedes beliebige Unternehmen mit eigener Softwareinfrastruktur kommt in Frage. Die Einschränkung der Rechte der eigenen Software spielt innerhalb eines Unternehmens im Allgemeinen eine untergeordnete Rolle. Bei großen Organisationen mit dezentraler IT (z.B. Ämter, Großunternehmen mit mehreren Länderniederlassungen) kann die Relevanz allerdings gegeben sein. Erfolgt der Zugriff auf die Services von privaten Geräten der MitarbeiterInnen, ist eine Einschränkung der Rechte der Applikation in jedem Fall gerechtfertigt.

Als Beispiel könnte eine mobile Zeiterfassung dienen, bei welcher der Aufenthaltsort der Person (ungefähr) erfasst werden soll. Dieser muss aus Komfortgründen automatisch erkannt werden. Dazu betreibt das Unternehmen entweder ein eigenes Trust Center für seine Anwendungen, oder es erwirbt das Zertifikat bei einer öffentlichen Zertifikatsstelle. Die mobilen Geräte der MitarbeiterInnen vertrauen entweder allen Sites dieser Zertifikatsstelle (hausinterne Zertifikatsstelle) oder allen Sites dieses Herstellers (öffentliche Zertifikatsstelle).

6.5 Trust Center Betreiber: Mobile Internet Access Provider

Während der Hersteller eines bestimmten Gerätes die Entwicklung proprietärer Software für sein Gerät favorisieren wird, kann es für den Netzanbieter (Vodafone, T-Mobile etc.) durchaus interessant sein, den eigenen KundInnen auf ihrem Providerportal Dienstleistungen anzubieten, die über reine Webapplikationen hinausgehen. Der Einsatz der TC^{3}AS-Architektur ist aus Kostengründen relevant. Zusätzlich bietet es sich für einen Netz-Provider an, ein Trust Center für seine KundInnen zu betreiben.

Das *Extensible Device API* der TC^{3}AS-Architektur könnte bei Vertragshandys des Providers auf neuen Geräten sogar vorinstalliert werden.

7 Fazit

Die Konfiguration von Sicherheitseinstellungen ist für viele AnwenderInnen nicht zumutbar. Aus diesem Grund muss auf Webapplikationen, die Zugriff auf das lokale System benötigen, bisher verzichtet werden. Das System der „Trust Center Controlled Code Access Security“, das in diesem Paper vorgestellt wird, löst die Problematik:

- Die Konfiguration der Sicherheitseinstellungen muss nicht für einzelne Applikationen getroffen werden. Stattdessen werden die Einstellungen für alle Applikationen einer gemeinsamen Klasse getroffen.
- Die Einteilung konkreter Applikationen in diese Purpose Classes erfolgt nicht durch die AnwenderIn, sondern durch den Anbieter der Applikation. Diese Einteilung muss durch eine vertrauenswürdige Instanz bestätigt werden.
- Das Promoter-Prinzip befreit die EndanwenderInnen davon, einzelnen unbekannten Applikationen vertrauen bzw. diese konfigurieren zu müssen.

Die Konfiguration beschränkt sich für den User damit darauf, Applikationen bestimmter Purpose Classes zuzulassen oder abzulehnen bzw. zu bestimmen, welche Applikation oder welcher Promoter als vertrauenswürdig eingestuft wird.

Diese Konfiguration kann bequem am PC durchgeführt und in einem Trust Center hinterlegt werden. Durch die Auswahl eines Trust Centers sowie Eingabe der User Credidentials wird das Sicherheitsprofil am mobilen Gerät übernommen.

Besucht die AnwenderIn eine neue Webapplikation, die von den erweiterten Möglichkeiten des im Paper dargestellten „Extensible Device API“ Gebrauch machen möchte, so muss diese Applikation ein digitales Zertifikat aufweisen, das die Identität des Anbieters bzw. der Applikation bescheinigt. Bevor die Applikation auf das lokale System Zugriff bekommt, wird das Zertifikat beim Trust Center automatisch überprüft. Ein Programm bekommt im Allgemeinen aber nie Zugriff auf alle Funktionen der Schnittstelle, sondern nur auf jene, die zur Erfüllung des Zwecks der Applikation (bestimmt durch die Purpose Class) notwendig sind.

8 Weiterführende und zukünftige Arbeit

Das geschilderte System der Trust Center Controlled Code Access Security ist im Konzeptionsstatus. Derzeit sind einige Details noch ungeklärt bzw. dienen als Anhaltspunkte für weiterführende Diskussionen:

- In welcher Form können Purpose Classes am besten identifiziert werden? Soll die Klassifizierung durch eine zentral entworfene Taxonomie erfasst werden oder kann sie durch eine Folksonomie gefunden werden. In welcher Form ist eine nachträgliche Erweiterung der Klassifizierung vorzusehen?
- Die meisten Desktop Browser verwenden ein Plug-In Konzept, das die Erweiterung des Browsers um das Extensible Device API zulässt. Als Referenz kann hier das Gears-API dienen. Browser von Mobiltelefonen können derzeit meist nicht durch Plug-Ins erweitert werden. Browser von Drittherstellern, welche das Extensible Device API implementieren, könnten den Lizenzbedingungen der Plattformhersteller widersprechen.
- Im vorliegenden Konzept kann nur der clientseitige Teil des Codes einer Anwendung signiert werden. Der Serverteil bzw. was mit den Daten am Server passiert, kann nicht durch eine Signatur gesichert werden. Hier kann der Hersteller nur auf Basis des Mission Statements rechtlich belangt werden, wenn er gegen die Vereinbarungen in seinem Mission Statement verstößt. Die rechtlichen Hintergründe (Gesetzeslage) müssen geklärt werden. Hier sind zudem regionale Unterschiede zu erwarten.

Unabhängig von den angeführten offenen Punkten bietet das Konzept der Trust Center Controlled Code Access Security für die potentiellen BenutzerInnen Erleichterung und Sicherheit beim Arbeiten mit Web Applikationen.

Literatur

[1] BARANAUSKAS, C. 2007. *Human-computer interaction - INTERACT 2007*. Springer.

[2] BLUMENSTEIN, K. und SCHMIED, G. 2010. Die vier Kernprobleme der mobilen Webentwicklung. *Proceedings of 3. Forum Medientechnik* (St. Pölten, Austria, 2010).

[3] BRAZ, C. und ROBERT, J.-M. 2006. Security and usability: the case of the user authentication methods. *Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine* (New York, NY, USA, 2006), 199–203.

[4] CRANOR, L.F. und GARFINKEL, S. 2005. *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc.

[5] ECKERT, C. 2009. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg Wissenschaftsverlag.

[6] File API: 2011. *http://dev.w3.org/2006/webapi/FileAPI/*. Accessed: 2011-06-06.

[7] Fire Eagle: 2007. *http://fireeagle.yahoo.net/*. Accessed: 2011-06-03.

[8] Gears API - Google Code: 2011. *http://code.google.com/intl/de-DE/apis/gears/*. Accessed: 2011-06-03.

[9] Gears API Blog: Hello HTML5: 2010. *http://gearsblog.blogspot.com/2010/02/hello-html5.html*. Accessed: 2011-06-06.

[10] Geolocation API Specification: 2010. *http://www.w3.org/TR/2010/CR-geolocation-API-20100907/*. Accessed: 2011-06-06.

[11] JENDRICKE, U. und GERD TOM MARKOTTEN, D. 2000. Usability meets security - the Identity-Manager as your personal security assistant for the Internet. *Proceedings of the 16th Annual Computer Security Applications Conference* (Washington, DC, USA, 2000), 344.

[12] KRIHA, W. und SCHMITZ, R. 2009. *Sichere Systeme: Konzepte, Architekturen und Frameworks*. Springer.

[13] Mozilla Labs» Blog Archive» Introducing Geode: 2008. *https://mozillalabs.com/blog/2008/10/introducing-geode/*. Accessed: 2011-06-03.

[14] Offline Web Applications: 2008. *http://www.w3.org/TR/2008/NOTE-offline-webapps-20080530/*. Accessed: 2011-06-06.

[15] SHNEIDERMANN, B. 1998. *Designing the user interface: strategies for effective human-computer interaction*. Addison-Wesley.

[16] VECCHIA, M.D. 2004. *Outsourcing, Managed Services, Application Service Providing*. BPX @ Dalla Vecchia GmbH.

[17] Web Storage: 2011. *http://dev.w3.org/html5/webstorage/*. Accessed: 2011-06-06.

FORENSISCHE ANALYSE VON SMARTPHONES

Stefan Langeder, Matthias Schrattenholzer,

Christopher Mallmann

Im folgenden Beitrag werden Regeln und Methoden diskutiert, wie man Daten, aus denen man Rückschlüsse auf den Nutzer eines Smartphones ziehen kann, erlangt, um diese anschließend auszuwerten. Dabei werden zuerst einige Richtlinien für die forensische Arbeit erläutert, anschließend wird jeweils die Analyse von SIM Karten und die Analyse des internen Speichers von Smartphones am Beispiel von Android behandelt.

1 Einleitung

Während die Nutzung des Internets stetig steigt, geht die Nutzung von klassischen Computersystemen zugunsten von Tablets und Smartphones merklich zurück. Diese neueren Geräte stellen - neben der Möglichkeit zu telefonieren - auch einen mobilen Zugriff auf das Internet zur Verfügung.

Mit einer schnell wachsenden Menge an verschiedensten Anwendungen, die für diese Geräte geschrieben und zu einem großen Teil frei zur Verfügung gestellt werden, werden Smartphones und Tablets immer mehr als portable Alternative zum Desktop Computer angesehen. Damit steigt auch der Druck auf die Forensik, da es immer wichtiger wird, Methoden zur Sicherstellung von Daten von diesen Geräten zu finden.

Bei der Analyse von Smartphones gibt es verschiedenste Daten, aus denen Rückschlüsse auf den Nutzer gezogen werden können. Darunter fallen zum einen Kontakte, SMS und das Anrufprotokoll, welche auch auf klassischen Handys und SIM Karten zu finden sind. Zum anderen gehören dazu Fotos, Videos, Tonaufnahmen, e-Mails, Browser-Verlauf und Geodaten, welche typischerweise auf Smartphones gefunden werden.

2 Richtlinien bei der forensischen Untersuchung von Smartphones

Um bei forensischen Untersuchungen die Integrität der Daten zu gewährleisten und somit auch die Beweise vor Gerichten verwenden zu können gilt es, sich an gewisse Richtlinien zu halten.

Die „Association of Chief Police Officers“, kurz ACPO (England, Wales und Nordirland), schlägt folgende Prinzipien vor, um dies zu garantieren [1]:

„Prinzip 1:

Die Strafverfolgungsbehörden oder deren Agenten dürfen keine Daten auf einem Speichermedium oder Computer verändern, wenn diese anschließend einem Gericht vorgelegt werden. Um dies zu garantieren, muss man das mobile Gerät nach der Beschlagnahme vom Netzwerk isolieren.

Eine Möglichkeit wäre es das Gerät auszuschalten, was allerdings voraussetzt, dass man Authentifizierungscodes wie den SIM-Code oder den Geräte-Sicherheits-Code weiß um anschließend wieder Zugang zu dem Gerät zu bekommen oder diesen vom Service-Provider anfordert. Nur in Fällen wo eine Verzögerung inakzeptabel ist oder Lebensgefahr droht sollte der Rat eines Spezialisten eingeholt werden; erst nachdem dieser die Situation beurteilt hat, sollte weitergemacht werden. Sollte das Gerät Zugang zum Netzwerk haben, so besteht einerseits die Gefahr von geplanten Skripten, die Daten auf diesem löschen und unerreichbar machen, aber auch die Lebensdauer des Akkus wird deutlich reduziert. Eine andere Möglichkeit das Gerät vom Netz zu trennen ist, es zu isolieren. Ein hierzu vorgeschlagenes aber nicht empfohlenes Mittel ist das Verwenden eines Störsenders. Dies ist in einigen Ländern verboten und es kann auch mit anderen Netzwerken zu Interferenzen kommen. Empfohlen wird hier eher die Verwendung eines abgeschirmten Raumes. Da die Kosten hierfür sehr hoch ausfallen können wird ein „faradaysches Zelt“ als die kostengünstigere und mobilere Lösung empfohlen. Auch beim Transport des Gerätes ist natürlich darauf zu achten die Isolation aufrecht zu erhalten, wie zum Beispiel unter Verwendung einer abgeschirmten Box. Ein weiteres Mittel, um das mobile Gerät vom Netzwerk abzuschirmen, ist die Benutzung einer sogenannten „Access Card“, eine SIM Karte die die originale SIM Karte simuliert, aber den Zugang zu jeglichen Netzen verwehrt. Zuletzt kann noch eine Anfrage beim Service Provider gestellt werden, der den Account des Benutzers sperren kann, wenn dieser kooperiert. Der Nachteil an dieser Methode ist, dass Nachrichten auf der Mailbox ab diesem Moment nicht mehr erreichbar sind. Des Weiteren darf zur Untersuchung des Gerätes nur Software, die für forensische Untersuchungen konzipiert ist, verwendet werden. Die meisten anderen Tools gelangen über das Betriebssystem an Daten und somit ist ein 2-Wege Transfer unvermeidlich. Sollte man wirklich auf diese Tools zurückgreifen müssen, so sollten diese zumindest im Vorhinein in der gleichen Umgebung schon einmal getestet worden sein und die resultierenden, möglichen Änderungen am Gerät bekannt sein. Ein solcher Prozess sollte so spät wie möglich durchgeführt werden. Bei der Wahl der Verbindung zu dem Gerät ist das Kabel die beste Entscheidung. Dieses ist in der Regel zuverlässig und hat die geringsten Auswirkungen auf das Gerät selbst. Infrarot ist weniger sicher, unzuverlässiger und verlangt normalerweise Interaktionen mit dem Gerät. Der unsicherste Zugang, hinsichtlich der Integrität der Daten, zu dem Gerät ist Bluetooth, da hier Daten während des Authentifikationsvorganges auf das Gerät geschrieben werden.

Der Zugriff über WLAN Schnittstellen wird in absehbarer Zukunft möglich sein. Die/der Untersuchende soll auch akzeptieren, dass manche Daten bei der Untersuchung verändert werden. Eine gelesene Nachricht soll jedoch nicht ungelesen gemacht werden, sondern das Lesen, oder das Ändern eines Status soll protokolliert werden, sodass jeder Vorgang für Außenstehende nachvollziehbar ist. Der Untersuchungsprozess selbst soll genau geplant sein, um somit Datenverlust zu vermeiden. Die Abfolge der Untersuchung (Gerät – SIM Karte) hängt von vielen Faktoren, die vielleicht den ganzen Fall betreffen, ab. So erfordert das Entnehmen der SIM Karte bei den meisten Geräten das Herausnehmen des Akkus, was wiederum ein Abschalten des Gerätes zur Folge hat. Dies kann zum Verlust von Zeit und Daten führen. Um die Ergebnisse der Untersuchung unter Verwendung forensischer Software zu verifizieren, sollte das Gerät auch manuell untersucht werden. Um hier aber keine großen Veränderungen am Gerät selbst zu machen, sollten sich die Untersuchenden mit einem gleichen Gerät vertraut machen oder das Benutzerhandbuch lesen. Beim Umgang mit der PIN (Personal Identification Number) gilt es besonders acht zu geben. Der erste Schritt sollte sein die verbleibenden Eingabeversuche für die PIN und PUK (Personal Unlocking Key) mittels eines forensischen Tools herauszufinden. Es kann auch angemessen sein den Default PIN des Service Anbieters zu versuchen, um die Verzögerung bis zum Erhalt des PUKs zu verkürzen. Der PUK hingegen darf niemals „geraten“ werden, da nach 10 maliger Falscheingabe der Inhalt der SIM Karte nicht mehr gelesen werden kann.

Prinzip 2:

Auf die Daten eines Computers oder Mobilen Gerätes direkt zuzugreifen ist in erster Linie zu vermeiden, wenn dies jedoch trotzdem notwendig sein sollte, dann muss dies von einer fachlich kompetenten Person gemacht werden, die dann auch die Relevanz und Auswirkungen dieses Eingriffs erklären kann. Personen, die mobile Geräte zur Untersuchung bringen, müssen auf diesem Gebiet eingeschult sein und die nötigen Verpackungsmaterialien verwenden. Sie sollten sich auch bewusst sein, dass schon das bloße Wischen über das Display Änderungen mit sich bringen kann, im schlimmsten Fall Datenverlust. Es ist zwar noch nicht so weit verbreitet wie bei klassischen Computern, jedoch kann man Skripte oder Tools installieren die nach unsachgemäßer Handhabung eine Datenlöschung hervorrufen. Die untersuchenden Personen benötigen Ausbildung im Umgang mit mobilen Geräten und sollten Erfahrung mit ähnlichen Geräten und der Software beziehungsweise den Tools, die verwendet werden, haben. Dies ist vor allem dann relevant wenn bei der Verwendung nicht-forensischer Software eine Synchronisation mit dem Computer stattfindet und diese Änderungen hervorruft.

Prinzip 3:

Während des Untersuchungsprozesses sollten alle Schritte in einem Protokoll festgehalten werden. Ein Dritter, der den Prozess nachvollziehen will, sollte anhand dieses Protokolls zu den gleichen Ergebnissen kommen. Um dies zu gewährleisten, können vor und nach allen Schritten Fotos beziehungsweise Videos oder, Notizen über Informationen am Display zur Protokollierung gemacht werden. Des Weiteren sollten auch Änderungen, die am Gerät gemacht werden, wie zum Beispiel das Lesen einer Nachricht und somit das Ändern in den Status „gelesen", protokolliert werden. Die verwendeten Tools und deren Versionsnummer sollten ebenfalls im Protokoll vermerkt werden und dieses dann gemeinsam mit dem Schlussbericht eingereicht werden.

Prinzip 4:

Hier geht es um die organisatorische Abhandlung. Der/die verantwortliche Untersucher/in trägt Sorge dafür, dass die gesetzlichen Vorschriften und die hier beschriebenen Prinzipien eingehalten werden. Jede Person, die an der Untersuchung eines Mobilen Gerätes teilnimmt, muss eine Ausbildung in diesem Bereich haben und mit dem Gerät umgehen können. Weisungen vom „Investigation Officer" (Anm.: der Verantwortliche einer gesamten Untersuchung) müssen befolgt werden, da nur dieser die Wichtigkeit und Bedeutung einer einzelnen Untersuchung bewerten kann. „[9]

[9] Übersetzung: Matthias Schrattenholzer

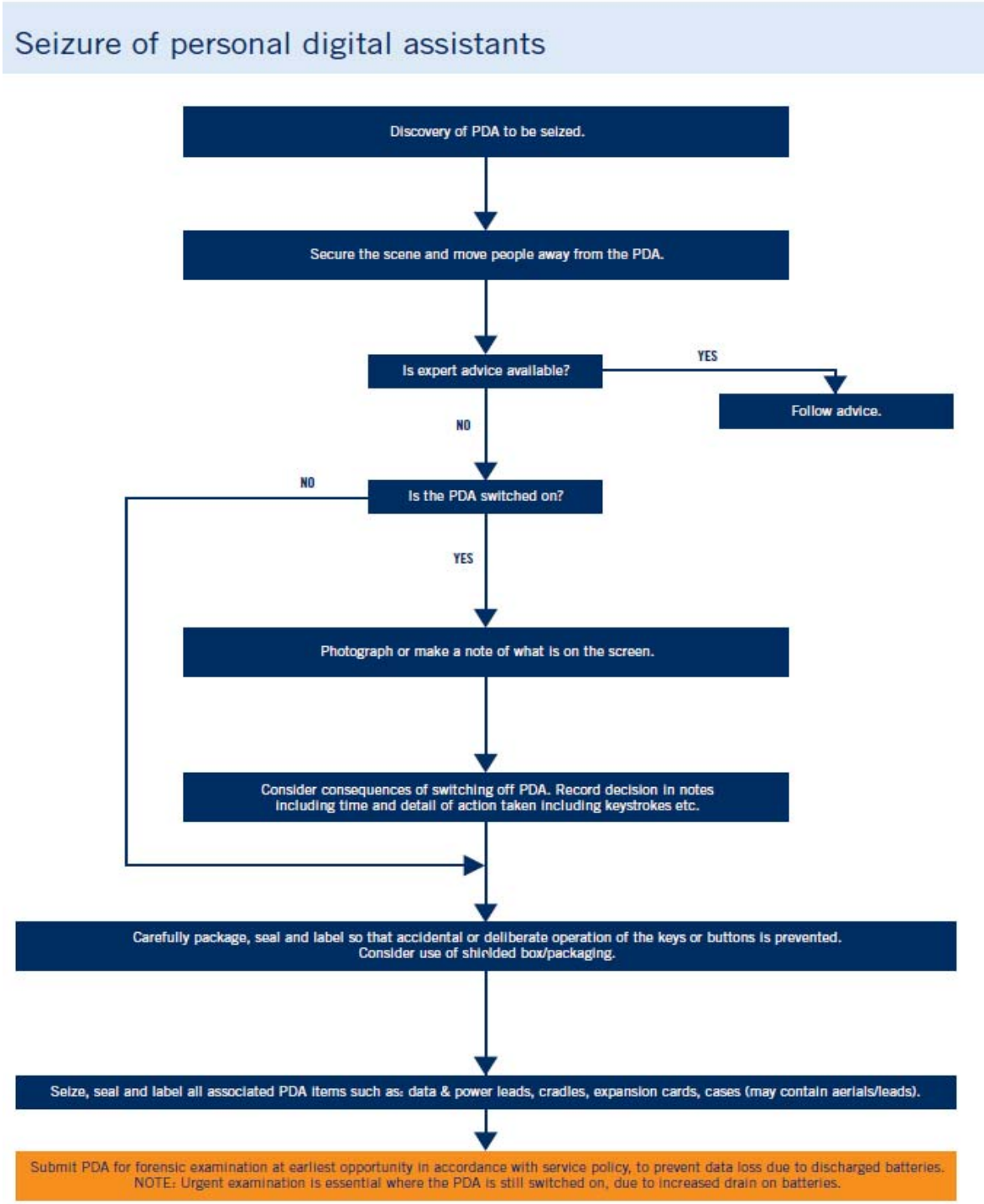

Seizure of personal digital assistants
Discovery of PDA to be seized.
Secure the scene and move people away from the PDA.
Is expert advice available?
YES
Follow advice.
NO
Is the PDA switched on?
NO
YES
Photograph or make a note of what is on the screen.
Consider consequences of switching off PDA. Record decision in notes including time and detail of action taken including keystrokes etc.
Carefully package, seal and label so that accidental or deliberate operation of the keys or buttons is prevented. Consider use of shielded box/packaging.
Seize, seal and label all associated PDA items such as: data & power leads, cradles, expansion cards, cases (may contain aerials/leads).
Submit PDA for forensic examination at earliest opportunity in accordance with service policy, to prevent data loss due to discharged batteries. NOTE: Urgent examination is essential where the PDA is still switched on, due to increased drain on batteries.

Abbildung 1: Ablauf von der Beschlagnahme eines Mobilen Gerätes bis zur Untersuchung [10]

[10] Quelle: Wilkinson, Sue (Hrsg.): The ACPO Good Practice Guide for Computer-Based Electronic Evidence, S.51 http://www.7safe.com/electronic-evidence/ACPO_guidelines_computer_evidence.pdf [23.9.2011]

3 Statistiken

Was die Verbreitung von Betriebssystemen angeht, ist man heutzutage im Bereich der Desktops folgende Situation gewohnt: Microsoft Windows liegt mit mehreren Versionen (XP, Vista und 7) im Bereich der Heim- und Arbeitsplatzcomputer mit Abstand vorne (ca. 88%-92% Marktanteil weltweit [2] [3]. An zweiter Stelle folgt Apples Mac OS X (ca. 5.3% - 5.6%), dahinter Linux und andere. Was die Serverwelt angeht, so liegen UNIX-Distributionen (ca. 64% [4]) vor Microsoft Windows (ca. 36% [4]).

Nun sieht die Situation in Sachen mobiler Betriebssysteme jedoch ganz anders aus: Im Gegensatz zur Welt der Desktops ist Windows eindeutig nicht das am weitesten verbreitete OS.

Aufgrund der vielen verschiedenen Hersteller allein von Smartphones teilen sich heute mehrere verschiedene, teils proprietäre Betriebssysteme den Markt. Aus diesem Grund ist es schwierig, sich einen eindeutigen Überblick über die Marktsituation zu verschaffen. Anders als bei manchen Themen gibt es große Abweichungen zwischen den Aussagen verschiedener Ratingfirmen – vor allem was Voraussagen oder Favorisierungen für die einzelnen Betriebssysteme am Markt betrifft.

Folgende Entwicklungen bilden sich jedoch in allen Reports und Prognosen ab: Während Symbian-Geräte immer seltener am Markt zu sehen sind, stieg Android als mobiles Betriebssystem im letzten halben Jahr rapide auf und wird derzeit auf gleicher Höhe mit – aber auch oft schon vor – Apples iOS favorisiert. Eine interessante Entwicklung ist das Rennen zwischen iOS und Android auf dem US-Markt: Im November 2010 stellte The Nielsen Company nach einer sechs Monate langen Beobachtung fest, dass Apple in Sachen verkaufter Smartphones im Allgemeinen zwar führt, jedoch Android-Geräte in diesen sechs Monaten die meisten Neukunden gewannen. [5]

International betrachtet sieht die Marktsituation derzeit so aus, dass Android Geräte sich nach wie vor ein knappes Rennen mit iOS Geräten liefern. Symbian, dass von Nokia nun scheinbar auf Eis gelegt wurde, da das Unternehmen fortan mit Microsofts Windows Phone 7 weitermachen wird [6] [7], verlor binnen einem Jahr fast die Hälfte seines Marktanteils (ca. 44% im Q1/2010, ca. 27% im Q1/2011). Microsoft selbst konnte auch in letzter Zeit am Markt der Smartphones mit Windows Phone 7 nur mittelmäßige Anteile einfahren, obwohl sich der Anteil mehr als verdoppelt hat (ca. 3,3% im Q1/2010, ca. 6,8% im Q1/2011). Interessant ist auch, dass gerade im Fall Microsoft sich die Marketing Experten scheinbar nicht wirklich einig sind, wenn es um Prognosen der Marktanteile geht. Während beispielsweise Gartner und IDC Microsoft im Jahr 2015 mit einem Marktanteil von jeweils ca. 19,5% [8] und 20,3% [9] sehen, blieb ABI Research bei ihrer Einschätzung und sagte für Microsoft einen Anteil von nur 7% voraus [10]. Auch für Research In Motions BlackBerry OS birgt der Markt in letzter Zeit viele Hürden. War es doch einst eines der populärsten mobilen Betriebssysteme, so fiel bereits letztes Jahr vor allem in den USA sein Marktanteil stark ab (41% im Q1/2010, 55% 2009 [11]). Derzeit sieht es am weltweiten Markt für RIM Geräte ähnlich aus (19,7% im Q1/2010, 12,9% im Q1/2011 [6]).

Die Tatsache, dass RIM seine BlackBerry Geräte ab 2012 mit dem QNX OS betreiben will, welches bereits für seine PlayBook Tablets verwendet wird [12], könnte die Geräte etwas tauglicher für den heutigen Smartphone Markt machen. Ob sich jedoch auch der Marktanteil damit verstärken lassen wird, bleibt abzuwarten – RIMs Marktanteil wird laut Prognosen jedenfalls bis 2015 bis auf etwas über 11% sinken [8], während QNX mit einem Anstieg von bisherigen 5,6% im Erscheinungsjahr 2011 auf 10% im Jahr 2015 [12] bessere Chancen berechnet werden.

Was die Frage nach der zukünftigen Marktsituation für Android Geräte angeht, so sind sich alle einig: mit einem derzeitigen Marktanteil von ca. 36-38,9% [6] [8] [9] wird es in den nächsten Jahren noch stärker vertreten sein. Im Jahr 2015 sieht man Android ganz vorne mit einem Anteil zwischen 43,8% [9] und 48,8% [8].

4 Analyse von GSM SIM Karten

4.1 Aufbau und Daten einer SIM Karte

Die GSM SIM Karte ist eine klassische Chip-Karte mit Sicherheitslogik. Wie alle Chipkarten besitzt sie ein Dateisystem, worin die Daten gespeichert werden. Sicherheitslogik bedeutet, dass zum Zugriff auf bestimmte Dateien die PIN erforderlich ist. Der Aufbau des Dateisystems (*Abbildung 1)* ist im GSM Standard 11.11 definiert [13].

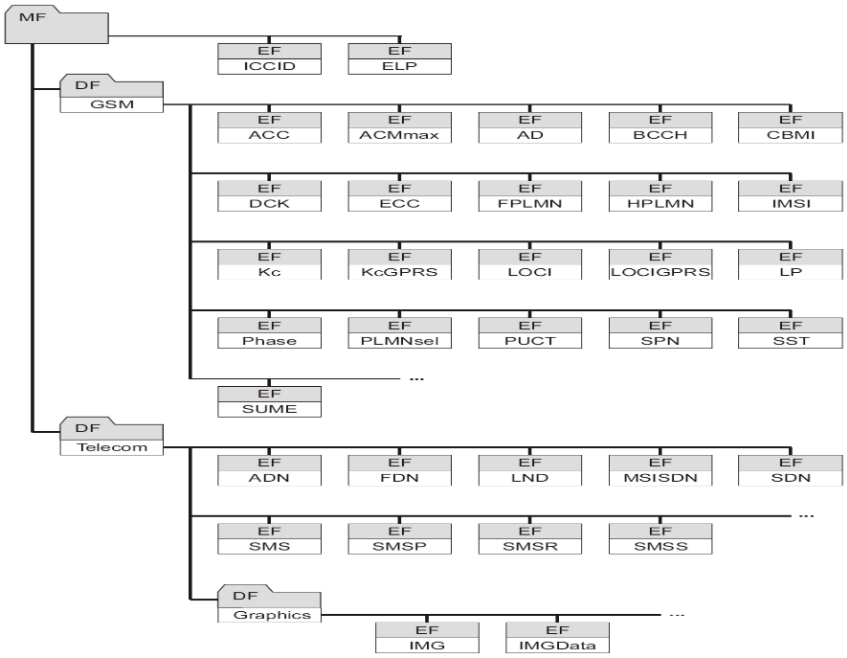


Abbildung 3: Dateistruktur einer GSM SIM Karte [13]

Aus diesen Dateien können nachfolgende Informationen gewonnen werden:

Service-Provider (EF/SPN): Diese Datei enthält den Namen des Service-Providers. Diese Daten können auch ohne PIN ausgelesen werden.

Kartenidentifikationsnummer (EF/ICCID): Die Kartenidentifikationsnummer ist weltweit einmalig. Anhand dieser Nummer kann vom Service-Provider der PUK angefordert werden. Diese Information kann auch ohne PIN ausgelesen werden.

IMSI (EF/IMSI): Die IMSI ist ebenfalls einmalig und dient zur Identifikation des Besitzers. Der Besitzer ist der, der den Kartenvertrag abgeschlossen hat. Der PIN ist zum Öffnen der Datei erforderlich.

Das Telefonbuch ist auf mehrere Dateien aufgegliedert. Zum Öffnen dieser Dateien ist jeweils die PIN erforderlich. Die Aufteilung der Dateien sieht folgendermaßen aus:

Telefonbuch (EFMSISDN und Erweiterungsdatei EXT1): Hier werden die Kontakte mit den zugehörigen Nummern gespeichert. Die Erweiterung dient zur Erhöhung der Speicherkapazität. Jeder Eintrag im Telefonbuch kann auf einen Eintrag in der Erweiterung verweisen. Desweiteren gibt es noch die zuletzt gewählten Nummern (*EFLND*) und die Kurzwahlnummern (*EFADN*). Zu diesen gehört jeweils die Erweiterung EXT1.

SMS (EF/SMS): Ebenfalls PIN erforderlich.

Eine weitere Datei, aus der Rückschlüsse auf vergangene Aufenthaltsorte des Nutzers gezogen werden können, ist die Datei *EF/PLMNSEL*. Darin werden die bevorzugten Provider anhand einer Identifikationsnummer gespeichert. Die ID ist wiederum so kodiert, dass sie einen Ländercode enthält. Der Ländercode ist in den ersten beiden Bytes dieser 3 Byte langen ID gespeichert.

Informationen über alle Dateien einer GSM SIM Karte können im GSM Standard 11.11 nachgelesen werden [13].

4.2 Methoden zum Auslesen der Daten

Der Zugriff auf die Daten der SIM Karte ist sowohl über ein Mobiltelefon als auch mit einem Kartenlesegerät mit entsprechender Software möglich. Einschränkungen beim Zugriff bestehen, wie bereits erwähnt, dadurch, dass gewisse Bereiche der SIM Karte durch die PIN geschützt sind. Die einzige Möglichkeit, diese Sperre zu umgehen ist jene, vom Service-Provider den PUK anzufordern.

Geeignete Software zum Auslesen von SIM Karten gibt es sowohl kostenpflichtig als auch im Open Source Bereich. Beispiele für beide Arten von Programmen sind Tulp2G, SimManager (TX Systems) und SIMCon (InsideOut Forensics).

Neben verschiedenen Programmen gibt es auch noch die Möglichkeit, die SIM Karte über ein Terminal und mit entsprechenden Kommandos auszulesen. Diese Methode ist allerdings äußerst aufwendig. Es muss eine genaue Reihenfolge beim Absetzen der Kommandos eingehalten werden [14]. Anschließend müssen die erhaltenen Informationen noch dekodiert werden. Die Kommandos selber müssen nach bestimmten Regeln zusammengestellt werden.

Eine Liste der möglichen Kommandos ist ebenfalls im GSM Standard 11.11 nachzulesen.

5 Extrahieren von Daten vom internen Speicher

Aufgrund der Hardwarearchitektur und Schutzmechanismen von Smartphones ist es nicht möglich, auf herkömmliche Weise ein Speicherabbild des internen Speichers zu erstellen. Mit Schutzmechanismen ist dabei ein Rechte-System gemeint, dass, im Falle von iPhone und Android, jenem von POSIX-Systemen entspricht. Im Bezug auf Hardwarearchitektur ist zu sagen, dass es durchaus Möglichkeiten gibt, eine bitweise Kopie des internen Speichers zu erstellen. Dies setzt jedoch den Einsatz spezieller Hardware voraus, weshalb wir im Verlauf unserer Arbeit nicht weiter darauf eingegangen sind.

Das Umgehen der Schutzmechanismen bedeutet am Beispiel Android, dass man sich zuerst Superuser-Rechte verschaffen muss. Für diesen Zweck gibt es eine Applikation, die es nach der Installation ermöglicht, alle anderen Applikationen als Superuser auszuführen.

Für unsere Untersuchungen haben wir, um einen Überblick über das Betriebssystem und den Aufbau von Android zu bekommen, anhand der Android Version *Android x86* (gedacht für Tablets) die Datenstruktur analysiert. Der größte Unterschied zu einem herkömmlichen Android auf einem Mobiltelefon ist jener, dass hier jeder Superuser sein kann, ohne Modifikationen am Gerät vornehmen zu müssen, und somit Zugriff auf alle Daten auf dem Gerät bekommt. Da unter Android x86 bei der Anwendung „Developer Tools“ ein Terminal Emulator installiert ist, kann man hier wie auf einem herkömmlichen Linux System arbeiten.

Um die gefundenen Dateien zu untersuchen, haben wir an diesen die Rechte geändert und in ein Verzeichnis kopiert, auf das später eine FTP-Client Applikation (Abbildung 4) Zugriff hat. Dieser Schritt war notwendig, da wir bei dieser Version von Android keine Möglichkeit gefunden haben, die verschiedenen Applikationen mit Superuser-Rechten zu starten. Am Ende wurden die Daten via FTP auf einen Rechner kopiert, auf dem die weitere Auswertung stattfand.

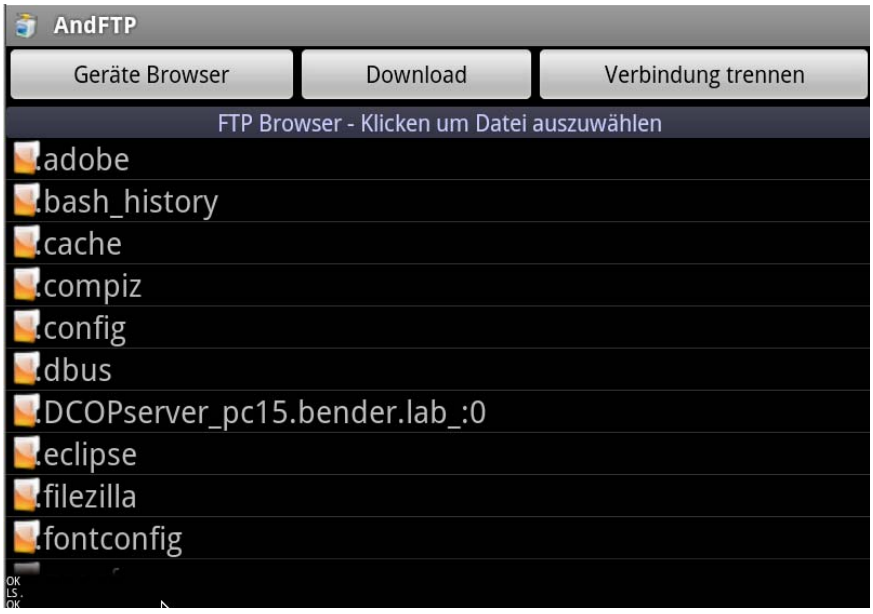


Abbildung 4: AndFTP, eine FTP Applikation für Android

Beispiele für fertige Lösungen von Programmen zum Extrahieren von Daten bietet zum Beispiel *Oxygen Forensics*. Hier werden, neben der eigentlichen Software, noch sämtliche Treiber und Suiten für eine breite Palette an Smartphones und Mobiltelefonen mitgeliefert. Die extrahierten Daten, wie zum Beispiel Geräteinformationen, Daten von der SIM Karte, jegliche Nachrichten, Webcache und Weblesezeichen werden dann übersichtlich zur Auswertung abgebildet.

Eine weitere Möglichkeit bietet viaExtract, eine Software die in Form einer virtuellen Maschine erhältlich ist und ähnlich wie Oxygen Forensics eine detaillierte Auswertung, jedoch nur von Android Geräten, liefert.

6 Auswerten der Daten

Die Auswertung der Daten des internen Speichers gibt je nach Betriebssystem vielfältige Informationen. Diese reichen von Kontaktlisten bis hin zum Wiederherstellen von gelöschten Dateien. [15]

Wichtig für das Auffinden der Daten ist, sich zuerst einen Überblick über die Dateistruktur des jeweiligen Betriebssystems zu verschaffen. Am Beispiel Android entspricht die

Dateistruktur jener von FreeBSD. Vom Root-Verzeichnis ausgehend navigiert man zu den gewünschten Dateien, um diese anschließend mit einem geeigneten Programm zu analysieren.

Bei unseren Experimenten haben wir herausgefunden, dass es unter Android ein Verzeichnis gibt, in dem alle Anwendungen ihre jeweiligen Ressourcen in Form einer SQLite Datenbank ablegen (*Abbildung 5*). Der Pfad des Verzeichnisses lautet */data/data*. Darin hat jede Anwendung einen Ordner, in welchem in einem weiteren Unterverzeichnis namens *databases* die Datenbank-Dateien liegen.

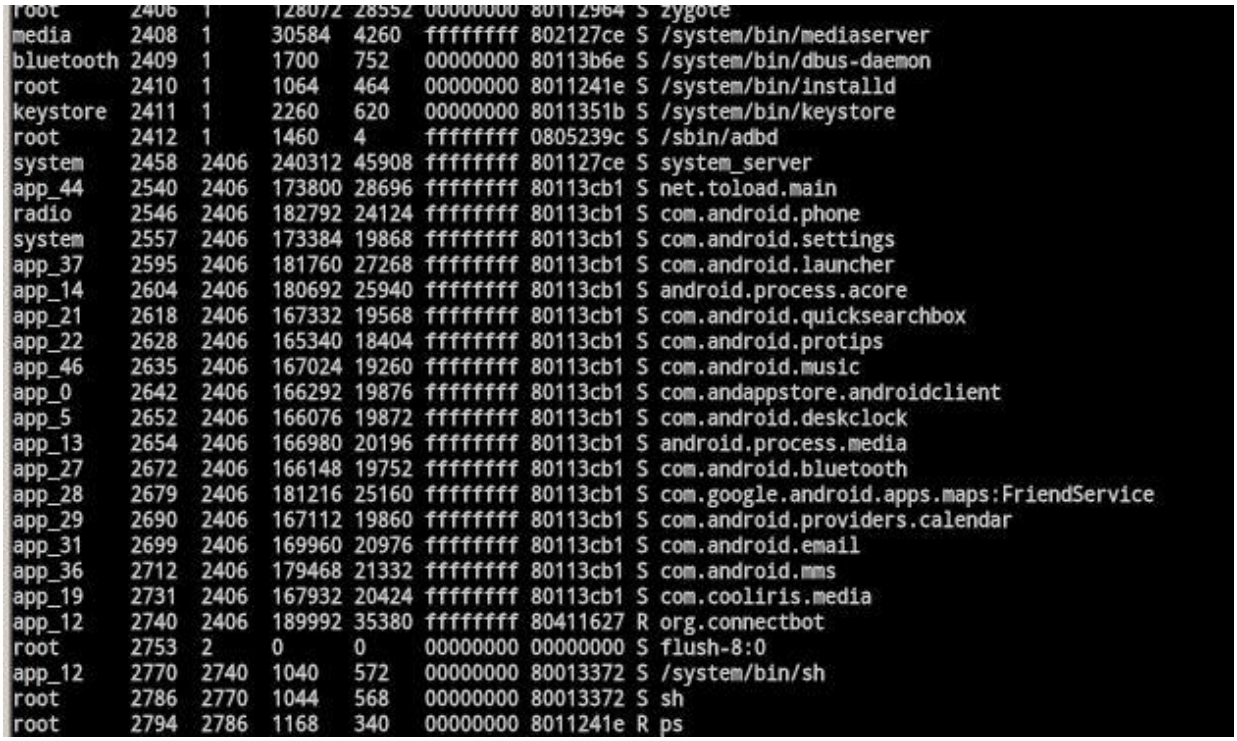

root 2406 1 128072 28552 00000000 80112964 S zygote
media 2408 1 30584 4260 ffffffff 802127ce S /system/bin/mediaserver
bluetooth 2409 1 1700 752 00000000 80113b6e S /system/bin/dbus-daemon
root 2410 1 1064 464 00000000 8011241e S /system/bin/installd
keystore 2411 1 2260 620 00000000 8011351b S /system/bin/keystore
root 2412 1 1460 4 ffffffff 0805239c S /sbin/adbd
system 2458 2406 240312 45908 ffffffff 801127ce S system_server
app_44 2540 2406 173800 28696 ffffffff 80113cb1 S net.toload.main
radio 2546 2406 182792 24124 ffffffff 80113cb1 S com.android.phone
system 2557 2406 173384 19868 ffffffff 80113cb1 S com.android.settings
app_37 2595 2406 181760 27268 ffffffff 80113cb1 S com.android.launcher
app_14 2604 2406 180692 25940 ffffffff 80113cb1 S android.process.acore
app_21 2618 2406 167332 19568 ffffffff 80113cb1 S com.android.quicksearchbox
app_22 2628 2406 165340 18404 ffffffff 80113cb1 S com.android.protips
app_46 2635 2406 167024 19260 ffffffff 80113cb1 S com.android.music
app_0 2642 2406 166292 19876 ffffffff 80113cb1 S com.andappstore.androidclient
app_5 2652 2406 166076 19872 ffffffff 80113cb1 S com.android.deskclock
app_13 2654 2406 166980 20196 ffffffff 80113cb1 S android.process.media
app_27 2672 2406 166148 19752 ffffffff 80113cb1 S com.android.bluetooth
app_28 2679 2406 181216 25160 ffffffff 80113cb1 S com.google.android.apps.maps:FriendService
app_29 2690 2406 167112 19860 ffffffff 80113cb1 S com.android.providers.calendar
app_31 2699 2406 169960 20976 ffffffff 80113cb1 S com.android.email
app_36 2712 2406 179468 21332 ffffffff 80113cb1 S com.android.mms
app_19 2731 2406 167932 20424 ffffffff 80113cb1 S com.cooliris.media
app_12 2740 2406 189992 35380 ffffffff 80411627 R org.connectbot
root 2753 2 0 0 00000000 00000000 S flush-8:0
app_12 2770 2740 1040 572 00000000 80013372 S /system/bin/sh
root 2786 2770 1044 568 00000000 80013372 S sh
root 2794 2786 1168 340 00000000 8011241e R ps

Abbildung 5: In diesem Verzeichnis liegen alle Ressourcen

Um die Dateien zu öffnen, wurden die Rechte so geändert, dass man diese in einem Unix System beliebig öffnen kann. Zum Öffnen wurde das Programm *SQLitebrowser* auf einem Ubuntu-Host verwendet. Da für die Untersuchungen nur die leere Tablet-Version von Android zur Verfügung stand, wurde für die Analyse nur ein Account für das bereits vorhandene Facebook-App erstellt. Außerdem wurde die Datenbankstruktur des Email-Programmes untersucht. Bei der Datenbank, die zum Facebook App gehört, fanden wir heraus, dass in dieser sowohl der Benutzername als auch das zugehörige Passwort im Klartext gespeichert werden. Die SQLite Dateien, die zum Email Programm gehören, ließen aufgrund der Tabellennamen schließen, dass in diesen sämtliche Emails mit allen dazugehörigen Informationen und Daten gespeichert werden. Desweiteren kann man aufgrund der Verzeichnisnamen und dem System, nach dem Daten abgelegt werden, davon ausgehen, dass auch viele andere brauchbare Informationen im Verzeichnis */data/data* zu finden sind.

Zu diesen Informationen gehören Browserverlauf, Kalenderinformationen und Kontaktinformationen sowie Geodaten. Es ist auch noch zu erwähnen, dass die SQLite Dateien anfänglich mit dem Unix Programm *find* gefunden wurden. Dieses kann ebenso für Fotos, Videos und Tonaufnahmen verwendet werden.

7 Zusammenfassung und Ausblick

Um vor Gericht ein mobiles Gerät wie ein Smartphone als handfestes Beweismittel zu etablieren gilt es sich an strikte Vorgaben zu halten. Die Vielfalt an Geräten, Betriebssystemen und die ständige Aktualisierung erfordert jedoch viel Know-How seitens der untersuchenden Person.

Die Analyse von SIM Karten bringt bereits einiges an Informationen mit sich. Allerdings ist es dabei notwendig, die PIN oder den PUK zu kennen, welcher dem Service-Provider bekannt ist.

Das Vorgehen beim Extrahieren von Daten, die am internen Speicher eines Smartphones liegen, ist vom jeweiligen Betriebssystem abhängig, und es gibt hierfür verschiedene Hard- und Softwarelösungen. In unserem Beispiel wurde ein Android Smartphone verwendet, und die Daten mit Hilfe von Softwareapplikationen extrahiert.

Um die richtigen Dateien zu bekommen, mussten diese zuvor im Verzeichnis gefunden werden. Dabei stellte sich ein gewisses System heraus, nachdem Daten, die von den jeweiligen Anwendungen verwendet werden, abgelegt werden. Aufgrund dieses Systems war es möglich, Rückschlüsse auf die generelle Verwaltung von Daten durch das Betriebssystem zu ziehen.

Der nächste Schritt bei unseren Forschungen zum Thema Smartphones wird sein, vollständige Abbilder des internen Speichers von Android- sowie auch iOS-basierenden Geräten zu erstellen. Danach kann versucht werden, durch verschiedene Filecarving-Techniken, gelöschte Daten wiederherzustellen. Desweiteren existiert eine Methode, um gelöschte Einträge in SQLite Datenbanken wiederherzustellen [16]. Auch diese werden wir auf die Datenbank Dateien von Smartphones anwenden.

Literaturverzeichnis

[1] Sue Wilkinson, "Good Practice Guide for Computer-Based Electronic Evidence," Association of Chief Police Officers,.

[2] o.V. (2011, Mai) Netmarketshare. [Online]. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd

[3] o.V. StatCounter Global Stats. [Online]. http://gs.statcounter.com/#os-ww-yearly-2008-2011-bar

[4] o.V. W3Techs. [Online]. http://w3techs.com/technologies/overview/operating_system/all

[5] o.V. nielsenwire. [Online]. http://blog.nielsen.com/nielsenwire/online_mobile/apple-leads-smartphone-race-while-android-attracts-most-recent-customers/

[6] Roberta Cozza et al. (2011, Mai) Gartner. [Online]. http://www.gartner.com/it/page.jsp?id=1689814

[7] Stephen Shankland. (2001, Februar) cnet News. [Online]. http://news.cnet.com/8301-30685_3-20031468-264.html

[8] Roberta Cozza. (2011, April) Gartner. [Online]. http://www.gartner.com/it/page.jsp?id=1622614

[9] o.V. IDC. [Online]. http://www.idc.com/getdoc.jsp?containerId=prUS22871611

[10] Don Reisinger. (2011, April) cnet News. [Online]. http://news.cnet.com/8301-13506_3-20051610-17.html

[11] ROBERT CYRAN and PETER THAL LARSEN. (2010, Juli) The New York Times. [Online]. http://www.nytimes.com/2010/07/26/business/26views.html

[12] Carolina Milanesi and Roberta Cozza. (2011, April) Gartner. [Online]. http://www.gartner.com/it/page.jsp?id=1626414

[13] European Telecommunications Standards Institute, "GSM Technical Specification," GSM 11.11, 2011.

[14] Wolfgang Effing Wolfgang Rankl, *Handbuch der Chipkarten*.: Carl Hanser Verlag, 2002.

[15] Jonathan Zdziarski, *iPhone Forensics*.: O'Reilly, 2008.

[16] Murilo Tito Pereira, "Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records," in *Digital Investigations Volume 5*, 2009, pp. 85-92.

FORENSISCHE UNTERSCHUNG MULTIMEDIALER DATEN

Rainer Poisel, Simon Tjoa

In diesem Dokument wird der Stand der Technik im Bereich der forensischen Analyse multimedialer Daten dargelegt. Immer größer werdende Datenmengen, sowie die Vielzahl an unterschiedlichen Multimediadaten und der starke Zeitdruck haben in den letzten Jahren zu großen Fortschritten im Bereich der Auswertung geführt. Der Vorteil für den Leser dieser Arbeit liegt darin, dass dieser straff zusammengefasst einen Überblick über den aktuellen Stand der Technik im Bereich der forensischen Untersuchung multimedialer Daten bekommt.

1 Einleitung

In unserer heutigen Informationsgesellschaft sind Computer nicht mehr wegzudenken. Die Zahl der elektronischen Geräte, wie z. B. tragbare Computer oder Smartphones, die uns während unserer täglichen Tätigkeiten unterstützt, nimmt, genau wie die zu verarbeitende Datenmenge, kontinuierlich zu. Diese Entwicklungen geben greifbare Argumente, warum auch die Verwendung von Computern zur Planung, Unterstützung und Durchführung krimineller Tätigkeiten im Wachsen begriffen ist. Das akademische Feld, das sich dieser Umstände im weitesten Sinne annimmt ist der Bereich der Informationssicherheit mit den Schwerpunkten Steganographie und digitale Forensik.

Im Jahr 2008 überstieg die Zahl der weltweit im Einsatz befindlichen Computer die Milliardenmarke [15]. Nationale Statistiken, wie z. B. die Polizeiliche Kriminalstatistik des deutschen Bundesministeriums des Innern zeigen, dass es hinsichtlich der begangenen Verbrechen, sowie der Aufklärungsrate gegenläufige Entwicklungen gibt: während die Zahl der Fälle vom Jahr 2009 auf das Jahr 2010 um 12% stieg, nahm die Aufklärungsrate um 1.7% ab [4]. Zufolge einer im Jahr 2010 durchgeführten Studie über Sicherheitslücken in IT Systemen (“Information Security Breaches Survey”, [29]) verzeichneten 92% der großen Unternehmen Sicherheitsvorfälle in ihrer IT Infrastruktur. Im Jahr 2008 war die Zahl noch um 20% kleiner. Mittlerweile müssen in 80 bis 90% aller Kriminalfälle digitale Beweismaterialien ausgewertet werden [22]. Aus diesem Grund ist es verständlich, dass seitens der Forschung und Entwicklung viel Aufwand in die Verbesserung der existierenden Methoden und Praktiken investiert wird.

Bei der Untersuchung multimedialer Daten handelt es sich um einen hochdynamischen Themenbereich. Die zeitlichen Rahmenbedingungen, die Vielzahl an verfügbaren Datenformaten,

sowie die immer steigenden Datenmenge führen dazu, dass ständiger Forschungsbedarf gegeben ist. Ein weiteres Problem stellen die kurzen Innovationszyklen dar. Diese erschweren das Schritthalten mit den in diesem Bereich stattfindenden Entwicklungen zusätzlich.

In diesem Zusammenhang sei der Unterschied zwischen der Multimedia und der Computer Forensik dargelegt: während sich die Computer Forensik in erster Linie mit den rohen digitalen Daten beschäftigt, hat die Multimedia Forensik die inhaltliche Analyse als Schwerpunkt [11]. Nichtsdestotrotz ist eine klare Trennung manchmal schwierig, da sich die Themenbereiche, vor allem im Bereich der inhaltsbasierten Datenwiederherstellung, stark überschneiden. Oft müssen die Ergebnisse aus beiden Disziplinen kombiniert werden, um die gewünschten Erfolge zu erzielen.

In diesem Dokument wird der Stand der Technik im Bereich der Analyse digitaler Multimediadaten dargestellt. Der Vorteil für die Leserin bzw. den Leser liegt daher darin, dass diese bzw. dieser sich rasch einen Überblick über die aktuellen Entwicklungen verschaffen kann. Das vorliegende Dokument behandelt die Auswertung multimedialer Daten (auditiv, visuell, video) und gliedert sich in zwei große Teilbereiche: die inhaltliche Analyse multimedialer Daten, sowie die Wiederherstellung multimedialer Daten von verschiedenen Datenträgern. Ähnliche Einteilungen der inhaltlichen Analyse multimedialer Daten können in [27] und [13] gefunden werden. Die inhaltsbasierte Datenwiederherstellung von verschiedenen Datenträgern wurde bereits in mehreren Publikationen diskutiert. Diese werden im entsprechenden Kapitel erläutert.

2 Inhaltliche Analyse multimedialer Daten

In diesem Kapitel werden die Teilbereiche der Untersuchung digitaler Multimediadaten erläutert. Oft finden sich bei der Analyse multimedialer Daten Parallelen zu Themenbereichen der klassischen Forensik. So ist beispielsweise die Identifizierung von Schusswaffen mit der Quellen-Identifizierung vergleichbar.

2.1 Quellen-Identifizierung

Die Quellen-Identifizierung („source identification“) wird eingesetzt, um das Gerät zu identifizieren, mit dem die zu analysierenden Aufnahmen gemacht wurden. Vergleichbar ist dieses Arbeitsfeld mit der Schusswaffenidentifizierung. Hier hinterlassen Geschosse Kratzer an Objekten, die von ihnen getroffen werden. Im Falle von Digitalkameras hinterlassen Sensoren und Optik ihre Spuren an den Aufnahmen.

Bei der Identifikation von Digitalkameras stehen mehrere Merkmale bereit: Eigenheiten der JPEG Kompression, die Farbfilter-Matrix („color filter array“, CFA), Fehlerstellen im Sensor und das Sensorrauschmuster („sensor pattern noise“, SPN).

In den meisten Publikationen werden mit dem Sensorrauschmuster die besten Ergebnisse erzielt. SPN wird meistens durch Unregelmäßigkeiten während der Herstellung beeinflusst. Unterschiedliche Pixel reagieren unterschiedlich auf unterschiedliche Lichtintensität aufgrund von Inhomogenitäten von Siliziumscheiben („silicon wafers“). Der Fingerabdruck einer Kamera wird als „Photo Response Non-Uniformity Noise“ (PRNU) bezeichnet. Die größte Herausforderung bei der Messung des SPNs liegt in der Kontaminierung dieses Musters mit Details aus der Umgebung.

Videokameras werden mit Hilfe von Technologien aus dem Bild- und Audiobereich identifiziert. Die Bildsensoren, die in Digital- und Videokameras eingesetzt werden, sind die Gleichen. Deswegen kann das Verfahren des Sensorrauschmusters auch hier angewandt werden. Mittlerweile existieren Verfahren, die selbst bei Anwendung einer starken Kompression das Quellgerät identifizieren können [31].

2.2 Umgebungsklassifizierung

Ermittler nutzen die Umgebungsklassifizierung („environment classification“), um den Ort, sowie die Umgebungsbedingungen von Aufnahmen zu bestimmen. Bei Bildern wird hierbei wiederum zwischen der Ereignis- und der Ortanalyse unterschieden. Bei beiden Verfahren wird das Ereignis bzw. der gezeigte Ort anhand der dargestellten Objekte klassifiziert [18], [19].

Auditive Informationen werden mit Hilfe von aus der Quellenidentifizierung bekannten Methoden nach ihrem Aufnahmeort und den Aufnahmebedingungen ausgewertet. Ein Beispiel für einen solchen Informationsträger ist die „Electrical Network Frequency“ (ENF). Das Signal wird durch das elektromagnetische Feld des Stromnetzes erzeugt und überlagert das Aufnahmesignal [16]. Zusätzlich werden Ansätze aus der Steganalyse eingesetzt, um diese versteckten Information zu ermitteln.

2.3 Inhaltsklassifizierung

Im Falle forensischer Analysen gilt es große Datenmengen innerhalb kurzer Zeit zu verarbeiten. Durch Automatisierung der Relevanzbestimmung soll bei der Inhaltsklassifizierung (“content classification”) eine Vorauswahl getroffen werden, damit die zu verarbeitende Datenmenge für den Menschen bewältigbar bleibt. Aufgrund der immer preiswerter werdenden Speichermedien hat die Informationsdichte je zu untersuchendem Speichermedium in den letzten Jahren rasant zugenommen.

Ein weiterer Grund für den Einsatz von Maschinen zur Inhaltsbestimmung liegt in der immer gleich bleibenden Wahrnehmung. Bei der Betrachtung durch Menschen muss berücksichtigt werden, dass diese bei längeren Arbeitssitzungen ermüden und die Auswertungsergebnisse je nach Tagesverfassung unterschiedlich ausfallen können.

Typischerweise setzen Ermittler Methoden der Inhaltsklassifizierung zur Identifizierung von nahezu allen Gegenständen und Lebewesen ein, die meisten Forschungsergebnisse wurden jedoch im Bereich der Klassifizierung von Bildern und Videos mit pornographischen Inhalten, sowie Material von Überwachungskameras und zur Klassifizierung von Beweisstücken bei Finanzdelikten (z. B. Schmuggel).

Bildern mit pornographischen Inhalten werden mit Hilfe der Hautfarbenerkennung klassifiziert [12]. Die Forscher nutzten als zusätzliches Merkmal bei der Klassifizierung den Dateinamen der zu analysierenden Dateien. Mit Hilfe dieser Vorgehensweise konnten Erfolgsraten von bis zu 95% erreicht werden. Bei einem weiteren Ansatz bei der Klassifizierung von Bildern, werden Bilder behandelt, als würden diese auf diskreten visuellen „Wörtern“ aufgebaut sein. Identifizierte Wörter werden in Form eines Histogrammes dargestellt um nach Anwendung von Filteralgorithmen festzustellen, wie sehr die gesuchten Inhalte vertreten sind. Voraussetzung für den Einsatz dieses Algorithmuses ist eine Trainingsdatenbank, die mit anwendungsspezifischen Daten gefüllt wurde. Videos erlauben neben der Klassifizierung von Objekten in Bildern die Analyse von Bewegungsabläufen [17].

2.4 Inhaltsfälschung

Die Inhaltsfälschung (“content forgery”) deckt Änderungen des Ursprungsmaterials auf. Auf diese Art lassen sich gefälschte Darstellungen von Sachverhalten aufdecken und nachweisen. Abbildung 2 zeigt ein erstes Beispiel, bei dem eine zusätzliche Rakete hinzugefügt wurde, um den gezeigten Inhalt medienwirksamer zu machen. Die als “copy-move forgery” bekannte Technik dupliziert Bildbereiche, um den in der Abbildung dargestellten Sachverhalt gezielt zu verändern. Es wurde mit Hilfe der von Popescu und Farid [28] vorgestellten Methodik untersucht. Bildinhalte, die mehrfach dargestellt werden, werden auf schwarzem Hintergrund weiß dargestellt. Auf diese Art sind die Änderungen für die menschlichen Sinne besonders einfach wahrzunehmen.

Abbildung 2: Bildmanipulation des “Iranian Missile Tests” und deren Erkennung [11]

Die von Popescu und Farid [28] vorgeschlagene Methodik wurde von Bayram et al. [9] verbessert, um auch nach einer erfolgten Nachbearbeitung kopierte Bildausschnitte erkennen zu können. Dazu werden die Fourier-Mellin Transform (FMT) Features herangezogen. Diese sind auch bei einer Skalierung und Verschiebung unverändert. Die Ergebnisse der Arbeit sind viel versprechend, da „copy-move“ Fälschungen auch dann erkannt werden können, wenn kopierte Teilausschnitte in bestimmten Bereichen rotiert (weniger als 10°), skaliert (weniger als 10%) oder stark komprimiert (besser als JPEG-Qualität 20) wurden.

Abbildung 3: Gefälschte Version des „Houston Crisis Rooms“ [7]

Weitere Bearbeitungsoperationen für digitales Bildmaterial sind:

- Retusche, um beispielsweise digitale Bilder ansprechender zu gestalten,
- teilweises Löschen unerwünschter Bildbereiche,
- Filtern unerwünschter Bildbereiche,
- Montage und Zusammenführen, um Bildbereiche aus unterschiedlichen Bildern zu kombinieren (auch bekannt als „image splicing“),
- Manipulation von Helligkeit, Farbraum und Kontrast und die
- Manipulation von Geometrie, um die Relation zwischen verschiedenen Objekten zu verändern.

Abbildung 4: Ausschnitt des “Houston Crisis Rooms” [7]

Abbildung 3 zeigt den „Houston Crisis Room“, wie er auf der Homepage von British Patrol (BP) gezeigt wurde. Bei näherer Betrachtung, siehe Abbildung 4, sind die Schnittkanten durch den starken Kontrastunterschied zwischen dem eingefügten Bildmaterial und dem Originalbild erkennbar. Bei dieser Fälschung handelt es sich um eine Anwendung des „Image Splicings“, die mit Hilfe von „Middle Level“ (Details siehe nachfolgend) Bildfälschungserkennungsalgorithmen erkannt werden können.

Abbildung 5: "High Level" Fälschungserkennung [1]

Die in den letzten Jahren erzielten Fortschritte bei den Bildfälschungserkennungsalgorithmen werden nach ihrer Komplexität eingeteilt [32]:

- Low Level: auf dieser Ebene werden Eigenheiten des Bildformates auf Unregelmäßigkeiten untersucht. Es werden keine semantischen Informationen ausgewertet. Zu diesen Eigenschaften zählen beispielsweise die DCT Koeffizienten oder Pixelwerte, die mit Hilfe statistischer Methoden ausgewertet werden.

- Middle Level: hier werden Spuren von verändernden Bearbeitungsoperationen mit Hilfe einfacher semantischer Information detektiert. „Splicing“, das scharfe Ecken verursacht, Unschärfeoperationen, die scharfe Ecken relativieren sollen, sowie Inkonsistenzen bei der Beleuchtung werden durch Verfahren in dieser Ebene erkannt.
- High Level: rein semantische Erkennungsmethoden kommen hier zum Einsatz. Die automatisierte Auswertung auf dieser Ebene setzt voraus, dass involvierte Personen korrekt identifiziert werden können. Weiters ist es notwendig, dass Kombinationen bewertet werden, ob sie realistisch auftreten können.

Die in Abbildung 5 dargestellte Bildfälschung würde beispielsweise durch „High Level“ Fälschungserkennung aufgedeckt werden, da hierbei politische Verhältnisse berücksichtigt und ausgewertet werden.

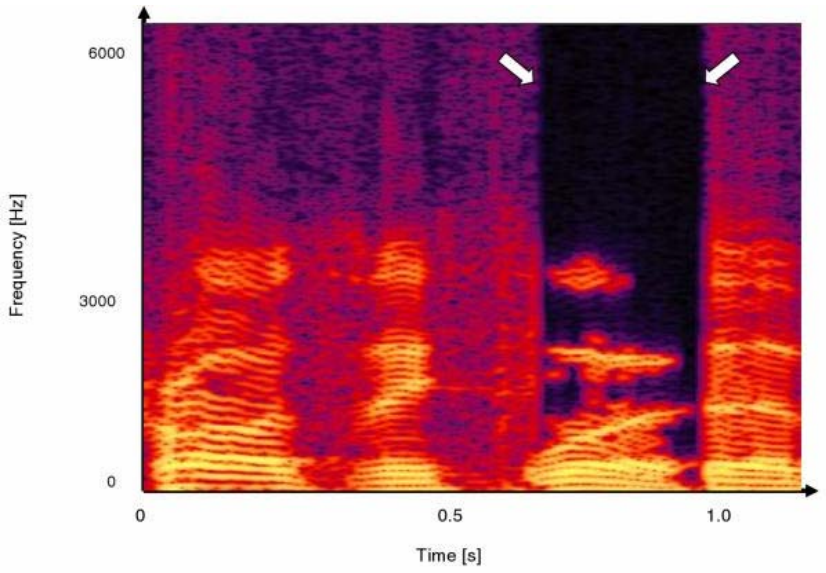


Abbildung 6: Veränderung des Spektrums bei Audiosignalen durch Austauschen von Ausschnitten [21]

Bei der Erkennung von Fälschungen bei auditiven Informationen muss der Untersucher visuelle, physikalische, elektrische und akustische Tests durchführen, die sicherstellen, dass die Rahmenbedingungen korrekt eingehalten werden [21]. Dazu zählen eine Überprüfung des chronologischen Verlaufs des Zustandekommens der Aufnahme, die Verifizierung des Aufnahmegeräts und dessen Eigenschaften, Mechanismen, die die Integrität des Aufnahmemediums sicherstellen, kritisches Gehör während der gesamten Aufnahme,

die Sicherstellung, dass die Aufnahme in einem Stück gemacht wurde und die Verwendung analytischer Werkzeuge, die Irregularitäten erkennen.

Eine Möglichkeit zur Erkennung von Modifikationen ist die „Electrical Network Frequency“ (ENF), die aufgenommene Audiosignale überlagert. Wird eine Aufnahme im Nachhinein verändert, so beeinflussen diese Änderungen auch die vom Stromnetz emittierten Frequenzen. In Abbildung 6 ist das Frequenzspektrum im Zeitverlauf ersichtlich. Die Änderungszeitpunkte werden durch die weißen Pfeile dargestellt. Im gezeigten Beispiel fehlen bei der modifizierten Information die Hintergrundgeräusche, die üblicherweise im hohen Frequenzbereich angesiedelt sind.

2.5 Steganographie und Steganalyse

Während sich die Kryptographie im Wesentlichen um den Schutz privater Daten kümmert, indem sie diese unkenntlich für Außenstehende macht, verschleiert die Steganographie zusätzlich die Existenz der geheim zu haltenden Informationen [23]. Bender et al. [10] stellte in ihrer Publikation vier wesentliche Ansätze zum Verstecken geheimer Information in auditiver und visueller Information fest. Diese Ansätze haben, obwohl bereits 15 Jahre alt, noch immer Relevanz:

- Low-bit coding: Nutzung des niederwertigsten Bits bei digital kodierter Information
- Echo hiding: Einbringen eines Echos mit variabler Verzögerung
- Phase coding: Verändern der Phasenlage von Signalen, sodass diese die geheime Information beinhaltet
- Spread spectrum: aufspreizen der geheimen Information; dieses geheime Signal wird mit unscheinbarer Trägerinformation überlagert.

Die Steganalyse kann als Gegenmaßnahme der Steganographie verstanden werden [20]. Hierbei wird zwischen signaturbasierten und zwischen statistischen Ansätzen unterschieden [23].

2.6 Standardisierung

Im Kontext der Forensik soll die Standardisierung genaue und zuverlässige Ergebnisse garantieren [33]. Wiles et al. teilen Standards in ihrer Publikation [33] in zwei Gruppen ein:

- Papier-Standards beschreiben die Menge an Vorgehensweisen der relevanten, forensischen Aktivitäten und
- Material-Standards, welche die zur Analyse notwendigen Werkzeuge spezifizieren.

Weiters wurden von den Regierungen verschiedener Länder Empfehlungen und Leitfäden herausgegeben, wie mit digitalem Beweismaterial umzugehen ist. In den Vereinigten Staaten veröffentlicht die "American Society of Crime Lab Directors/Laboratory Accreditation Board" (ASCLD/LAB) geeignete Regeln und Muster, um die Gültigkeit von Ergebnissen sicherzustellen [8]. In Großbritannien werden forensische Vorgehensweisen und Methoden seit 1999 von der "British Standards Institution" formalisiert [30]. Weitere Hinweise zum forensischen Analyseprozess gibt der "Good Practice Guide for Computer-Based Electronic Evidence" von der "Association of Chief Police Officers" (ACPO) [24]. In Deutschland veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik einen Leitfaden für Vorgänge in der IT-Forensik [5].

Zusammengefasst gab es in den letzten Jahren Fortschritte bei der Standardisierung von Dateiformaten, Schemen und Ontologien. Die größte Herausforderung im Bereich der Standardisierung stellt jedoch die Vereinheitlichung dar. Während relevante Prozesse und Ansätze bereits überformalisiert wurden, gibt es keinen universell (weltweit) gültigen Standard. Mögliche Ursachen sind die unterschiedlichen rechtlichen Lagen in den jeweiligen Ländern.

3 Wiederherstellung multimedialer Daten

Eng verbunden mit der forensischen Analyse ist die Wiederherstellung der auf Datenträgern gespeicherten Informationen ("data recovery"). Eine Übersicht über die Thematik wird bereits von Pal und Memon [6] gegeben. Je nach den der Analyse zugrunde liegenden Daten wird zwischen dateisystembasierender und inhaltsbasierter Wiederherstellung unterschieden.

3.1 Dateisystembasierende Wiederherstellung

Dateisysteme werden verwendet, um Daten auf Datenträgern in Form von Dateien, Verzeichnissen, Verweisen, etc. verwalten. Sind die Verwaltungsstrukturen vorhanden und ist es möglich, diese zu interpretieren, so können Dateien unabhängig von ihrem Inhalt wiederhergestellt werden. Dateisystembasierende Wiederherstellungsmethoden dienen oft auch als Basis für die inhaltsbasierte Datenwiederherstellung. Der Grund für diese Vorgehensweise liegt darin, dass nach einer Vorverarbeitung der Rechenaufwand für die inhaltsbasierte Datenwiederherstellung drastisch reduziert werden kann.

Werkzeuge, wie z. B. die open-source Software “The Sleuth Kit” (TSK [3]), sind in der Lage als gelöscht markierte Dateien, sowie Schlupfspeicher (“slack space”) oder unzugeordnete Speicherbereiche (“unallocated space”) zur weiteren Analyse, z. B. der inhaltsbasierten Auswertung, zu extrahieren.

3.2 Inhaltsbasierende Wiederherstellung

Stehen die Dateisystemstrukturen zur Wiederherstellung von Daten nicht bereit, so können die Dateiinhalte selbst zur Wiederherstellung herangezogen werden. Bei Verfahren, denen diese Informationen zugrunde liegen, wird im Wesentlichen zwischen der Wiederherstellung unfragmentierter und fragmentierter Dateien unterschieden.

Fragmentierung tritt beispielsweise auf, wenn der auf einem Datenträger zur Verfügung stehende Platz bereits zum größten Teil verbraucht ist, und die abgelegten Dateien bereits fragmentiert wurden [14]. Die Situation lässt sich anhand eines Beispiels verdeutlichen. Ist die größte Sequenz an zusammenhängenden, freien Clustern zehn, so wird eine Datei, die 14 Blöcke benötigt, in mindestens zwei Fragmente aufgeteilt: die zehn zur Verfügung stehenden Cluster für das erste Fragment, die verbleibenden vier Cluster werden auf weitere freie Speicherbereiche aufgeteilt. Die Reihenfolge, in welcher Speicherbereiche zugewiesen werden, ist abhängig von der jeweiligen Implementierung des Dateisystems. Weitere Gründe für das Auftreten einer Fragmentierung sind das Vergrößern existierender Dateien und so genannte „wear-leveling“ Algorithmen, die zum Einsatz kommen, um die Lebensdauer flash-basierter Datenträger zu erhöhen.

Die Wiederherstellung von Dateien auf Basis ihres Inhaltes wird durch „File Carver“ bewerkstelligt. Bei „File Carvern“ der ersten Generation wurde der Beginn und das Ende einer Datei anhand von Signaturen (Byte-Sequenzen) bestimmt: Diese „Header“ und „Footer“ sind abhängig vom wiederherzustellenden Dateityp und müssen nicht zwingend vorhanden sein. JPEG-Dateien zeichnen sich jedoch durch das Vorhandensein aus und können mit diesem Verfahren wiederhergestellt werden, sofern diese nicht fragmentiert abgelegt wurden.

Die Problematik der Fragmentierung kommt aber auch hier zum Tragen. Das Verfahren setzt voraus, dass die wiederherzustellenden Dateien nicht fragmentiert und damit der Inhalt sequentiell vorliegt. Die Entwicklungsschritte zur Wiederherstellung fragmentierter Text- und Bilddateien wurden von Pal und Memon dargestellt [6].

Anhand der von Garfinkel aufgestellten Statistik über die Fragmentierung von Dateien auf Datenträgern wurde das Verfahren des „Bifragment Gap Carvings“ entwickelt. Den Ergebnissen der Studie [14] zufolge werden Dateien häufig (z. B. ca. 3% der analysierten JPEG- und HTML-Dateien, 9% der analysierten PST-Dateien), in nur zwei Fragmente unterteilt.

Beim „Bifragment Gap Carving“ wird die Lücke zwischen den zwei Fragmenten einer Datei so lange variiert, bis ein Prüfalgorithmus die wiederhergestellte Datei dekodieren kann. Der Prüfalgorithmus kann beispielsweise ein JPEG-Dekodierer sein. In Abbildung 7 entspricht die Lücke zwischen den beiden Fragmenten den Clustern 304 und 305. Diese kann beispielsweise auf die Cluster 306 und 303 ausgeweitet werden.

Eine wesentliche Beschränkung für diesen Ansatz ist jedoch, dass eine inkorrekte Dekodierung anhand der Erfolgsmeldung des Dekodierers oft nicht von einer korrekten unterscheidbar ist.

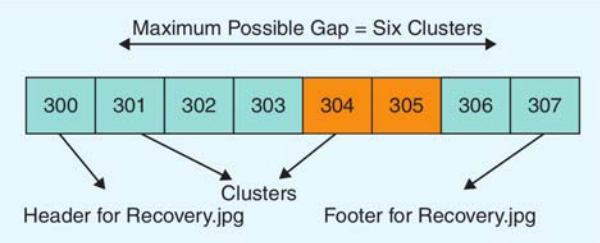


Abbildung 7: Bifragment Gap Carving [6]

Um die Problematik der inkorrekten Dekodierung in den Griff zu bekommen, führten Memon und Pal Wiederherstellungsverfahren ein, die auf den „Greedy“-Algorithmen der Graphentheorie beruhen [26]. Im Gegensatz zum „Bifragment Gap Carving“ können mit diesem Verfahren auch Dateien wiederhergestellt werden, die in mehr als 2 Fragmente aufgeteilt wurden. Das Zusammenpassen von Fragmenten wird mit Hilfe einer Gewichtung bewertet. Die Wiederherstellung läuft in mehreren Durchläufen ab. Ausgehend von den Basisfragmenten der wiederherzustellenden Dateien wird in jedem Durchlauf die beste Zusammengehörigkeit gespeichert und die betroffenen Fragmente als wiederhergestellt markiert. Die Durchläufe werden wiederholt, bis alle Fragmente Dateien zugeordnet wurden. Sequential Hypothesis Testing - Parallel Unique Path (SHT-PUP) [25] geht noch einen Schritt weiter und setzt voraus, dass Fragmente nicht aus der minimalen Blockgröße (ein Sektor, 512 Byte) bestehen. Im Gegensatz zur graphenbasierten Wiederherstellung wird in diesem Fall davon ausgegangen, dass Fragmente generell aus einer Vielzahl an Blöcken bestehen und Dateien im Wesentlichen aus einer geringen Zahl an Fragmenten bestehen (z. B. 3 Fragmente).

SmartCarving [6] kombiniert die bisher vorgestellten Verfahren des „File Carvings“ mit Elementen der dateisystembasierten Wiederherstellung von Dateien.

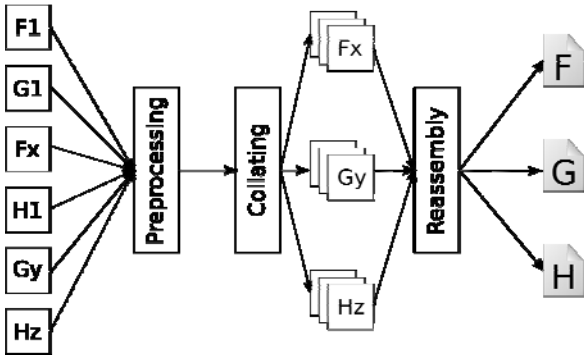


Abbildung 8: Architektur des SmartCarvings [6]

Wie in Abbildung 8 erfolgt die Wiederherstellung bei diesem Ansatz in drei Stufen:

- *Preprocessing*: In diesem Schritt erfolgt die Aufbereitung des Ursprungsmaterials, sodass es durch forensische Verfahren wiederhergestellt werden kann. Beispiele sind in diesem Fall die Entschlüsselung verschlüsselter Datenträger oder die Dekomprimierung komprimierter Datenträger. Weiters können in diesem Schritt die vom Dateisystem adressierbaren Datenblöcke identifiziert und von weiteren Bearbeitungsschritten ausgeschlossen werden. In der Abbildung werden die relevanten Fragmente unterschiedlicher Dateien (z. B. F, G, H) unabhängig von ihrer tatsächlichen Reihenfolge (1, 2, …, x, y, z) an den SmartCarver übergeben.
- *Collating*: Die Identifikation von Fragmenten passiert während der zweiten Phase. Dabei können relevante Blöcke durch das Auffinden von Signaturen (Bytefolgen) oder durch statistische Analysen ausfindig gemacht werden. Der signaturbasierte Ansatz eignet sich besonders zur Identifikation von Basisfragmenten, die den Anfang einer relevanten Datei anzeigen. Die identifizierten Blöcke werden durch nachfolgende Bearbeitungsschritte in die ursprüngliche Reihenfolge gebracht.
- *Reassembling*: Im letzten Bearbeitungsschritt hängt die Vorgehensweise stark vom Typ der wiederherzustellenden Daten ab. Dateifragmente werden an den beim „Collating“ ausgemachten Fragmentierungspunkten („fragmentation points“) zusammengesetzt (z. B. mit Hilfe des SHT-PUP Verfahrens) und auf ihre Dekodierbarkeit geprüft. Ist eine Dekodierung möglich, so erfolgt zusätzlich eine inhaltliche Analyse. Bei uneindeutigen Ergebnissen wird der Benutzer mit den zur Auswahl stehenden Möglichkeiten konfrontiert.

Im Bereich der Wiederherstellung von Digitalbildern konnten bereits große Fortschritte erzielt werden.

Das Programm „Adroit Photo Forensics 2011“ [2] kostet derzeit 1.000 US$ und unterstützt die Wiederherstellung mit „Smart Carving“ von Bilddateien im JPG, PNG, BMP, TIFF und in diversen RAW-Formaten. Letzteres Format ist herstellerabhängig und wird von diversen Digitalkameras benutzt, um Rohdaten abzulegen.

Momentan wird die Wiederherstellung von Videodaten erforscht. Eine wesentliche Herausforderung in diesem Bereich ist die große Zahl an zur Verfügung stehenden Videoformaten. Die aktuell durchgeführten Forschungsarbeiten erfolgen in mehreren Schritten:

- Wiederherstellung von Einzelbildern: „Ganzbilder“ oder „Intra-Frames“
- Wiederherstellung von Einzelbildern: „Zwischenbilder“ oder „Inter-Frames“
- Wiederherstellung von Videosequenzen

Einzelne Videofragmente werden anhand von Signaturen (Basisfragmente) und statistischer Analyse erkannt. Bei der statistischen Analyse kann davon ausgegangen werden, dass auch Daten in anderen Formaten (z. B. andere stark komprimierte Inhalte, wie z. B. JPG-Fragmente) als Videodaten klassifiziert werden. So genannte „False-Positives“ werden während der „Reassembly“ als ungültig klassifiziert und aus dem Wiederherstellungsprozess ausgeschlossen.

Ähnliche Überlegungen gibt es bei der Wiederherstellung von text-basierten Daten, wie z. B. HTML- und SVG-Dokumenten, sowie E-Mails. Hier kommen Algorithmen und Vorgehensweisen aus der Linguistik zur Anwendung [6].

4 Zusammenfassung und Ausblick

In diesem Dokument wurde der aktuelle Stand der Technik im Bereich der forensischen Analyse von digitalen Multimediadaten dargelegt. Neben der inhaltlichen Analyse solcher Daten wurde auf die Wiederherstellung von Datenträgern eingegangen.

Aufgrund der weiter steigenden Speicherkapazität sowie der immer günstiger werdenden Massenspeicher ist weiter mit einem Anstieg an auszuwertendem Material zu rechnen. Dies und der bei forensischen Untersuchungen herrschende Zeitdruck werden in diesem Bereich zu Fortschritten führen und rechtfertigen den momentan getriebenen Forschungsaufwand. Vor allem im Bereich der inhaltsbasierten Wiederherstellungsverfahren ist in nächster Zukunft noch mit Verbesserungen zu rechnen. Momentan existieren noch keine Ansätze, die auf die Wiederherstellung auditiver Information spezialisiert sind. Im Bereich von Videodaten wird im Moment die Machbarkeit abgeschätzt.

Literatur

[1] http://www.prisonplanet.com/images/february2006/280206bushbinladen.jpg. [Online; Status: June 15th 2011].

[2] Adroit photo forensics 2011. http://digital-assembly.com. [Online; Status 10/06/2011].

[3] The Sleuth Kit (TSK). http://www.sleuthkit.org/sleuthkit/. [Online; Status: April 15th 2011].

[4] Polizeiliche Kriminalstatistik 2010. http://www.bka.de/pks/pks2010/startseite.html, Mai 2010. [Online; Status: 25. Mai 2011].

[5] Leitfaden „IT-Forensik“, März 2011. [Online; Status: 26. Mai 2011].

[6] Nasir D. Memon Anandabrata Pal. The evolution of file carving. IEEE Signal Processing Magazine, March 2009:59 – 71, 03 2009.

[7] John Aravosis. FLASHBACK: BP photoshops fake photo of oil spill crisis command center to make it look busy. http://www.americablog.com/2010/07/bp-photoshops-fake-photo-of-command.html, April 2011. [Online; Status: June 15th 2011].

[8] ASCLD. Ascld (american society of crime lab directors/laboratory), 03 2011.

[9] Sevinc Bayram, Husrev Taha Sencar, and Nasir Memon. An efficient and robust method for detecting copy-move forgery. In Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP ’09, pages 1053–1056, Washington, DC, USA, 2009. IEEE Computer Society.

[10] W. Bender, D. Gruhl, N. Morimoto, and Aiguo Lu. Techniques for data hiding. *IBM Syst. J.*, 35:313–336, September 1996.

[11] Rainer Böhme, Felix C. Freiling, Thomas Gloe, and Matthias Kirchner. Multimedia forensics is not computer forensics. In *IWCF*, pages 90–103, 2009.

[12] Mateus de Castro Polastro and Pedro Monteiro da Silva Eleuterio. Nudetective: A forensic tool to help combat child pornography through automatic nudity detection. In *DEXA Workshops*, pages 349–353, 2010.

[13] Jochen Fürch and Johannes Meyer. Digitale multimediaforensik. Technical report, TU-Darmstadt, 2010.

[14] Simson L. Garfinkel. Carving contiguous and fragmented files with fast object validation. *Digital Investigation*, 4(Supplement 1):2 – 12, 2007.

[15] Gartner/Reuters. Computers in use pass 1 billion mark: Gartner. http://www.reuters.com/article/2008/06/23/-us-computers-statistics-idUSL2324525420080623, June 2008. [Online; Status: March 29th 2011].

[16] C. Grigoras. Digital audio recording analysis the electric network frequency criterion. Technical Report Application Notes, AN-4, Diamond Cut Productions, Inc., 2003.

[17] Christian Jansohn, Adrian Ulges, and Thomas M. Breuel. Detecting pornographic video content by combining image features with motion information. In *ACM Multimedia*, pages 601–604, 2009.

[18] Li-Jia Li and Li Fei-Fei. What, where and who? classifying events by scene and object recognition. *Computer Vision, IEEE International Conference on*, 0:1–8, 2007.

[19] Jiebo Luo, Wei Hao, Dale McIntyre, Dhiraj Joshi, and Jie Yu. Recognizing picture-taking environment from satellite images: A feasibility study. In *ICPR*, pages 1–4, 2008.

[20] S Lyu and H Farid. Steganalysis using higher-order image statistics. *IEEE Transactions on Information Forensics and Security*, 1(1):111–119, 2006.

[21] Robert Maher. Overview of audio forensics. In Husrev Sencar, Sergio Velastin, Nikolaos Nikolaidis, and Shiguo Lian, editors, *Intelligent Multimedia Analysis for Security Applications*, volume 282 of *Studies in Computational Intelligence*, pages 127–144. Springer Berlin / Heidelberg, 2010.

[22] Kim Medaris and Rick Mislan. Expert: Digital evidence just as important as dna in solving crimes, April 2008.

[23] Arooj Nissar and A.H. Mir. Classification of steganalysis techniques: A study. *Digital Signal Processing*, 20(6):1758 – 1770, 2010.

[24] Association of Chief Police Officers (ACPO). Good practice guide for computer-based electronic evidence. http://7safe.com/electronic_evidence/index.html.

[25] Anandabrata Pal, Husrev T. Sencar, and Nasir Memon. Detecting file fragmentation point using sequential hypothesis testing. *Digital Investigation*, 5(Supplement 1):S2 – S13, 2008. The Proceedings of the Eighth Annual DFRWS Conference.

[26] Anandrabatha Pal and Nasir D. Memon. Automated reassembly of file fragmented images using greedy algorithms. *IEEE Transactions on Image Processing*, 15(2):385–393, 2006.

[27] Rainer Poisel and Simon Tjoa. Forensics investigations of multimedia data: A review of the state-of-the-art. In *Proceedings of the 6th International Conference on IT Security Incident Management & IT Forensics*, 2011.

[28] Alin C Popescu and Hany Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Dartmouth College, Computer Science, 2004.

[29] PricewaterhouseCoopers. Information security breaches survey. Technical report, Infosecurity Europe, 2010.

[30] A. Shipman and British Standards Institution. *Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008.* British Standards Institution, 2008.

[31] Wiger van Houten and Zeno Geradts. Source video camera identification for multiply compressed videos originating from youtube. *Digital Investigation*, 6(1-2):48–60, 2009.

[32] Wei Wang, Jing Dong, and Tieniu Tan. A survey of passive image tampering detection. In Anthony Ho, Yun Shi, H. Kim, and Mauro Barni, editors, *Digital Watermarking*, volume 5703 of *Lecture Notes in Computer Science*, pages 308–322. Springer Berlin / Heidelberg, 2009.

[33] Jack Wiles, Tammy Alexander, Stevee Ashlock, Susan Ballou, Larry Depew, Greg Dominguez, Art Ehuan, Ron Green, Johnny Long, Kevin Reis, Amber Schroader, Karen Schuler, and Eric Thompson. Murder and money: The story of standards, accreditation, and certification in computer forensics. In *Techno Security's Guide to E-Discovery and Digital Forensics*, pages 261 – 276. Syngress, Burlington, 2007.

WAS WISSEN WIR ÜBER MALWARE?

Dr. Otto HELLWIG

Programme, die unerwünschte Effekte bei elektronischen und elektronisch gesteuerten Geräten erzeugen, sind Teil unseres Alltags geworden. Anders als bei sonstigen „Incidents“ (etwa bei Autounfällen) ist das verfügbare Wissen über Verursacher, Auftreten und Schäden von Malware sehr bruchstückhaft bzw. unvollständig. Der vorliegende Beitrag gibt einen Überblick über den aktuellen Wissensstand.

1 Einleitung

Malware gehört mittlerweile zum Alltag vieler Menschen, sei es aufgrund eigener negativer Erfahrungen, sei es durch die Berichterstattung der Medien[11]. Trotzdem gibt es relativ wenig strukturiertes Wissen über Malware. Auf der einen Seite sind sehr technische Unterlagen (z.B. bei IT-Sicherheits-Firmen) bzw. wissenschaftliche Ergebnisse verfügbar, auf der anderen Seite Artikel in Tageszeitungen oder Magazinen, die eher allgemeine Informationen liefern.

Es existieren mittlerweile sehr umfangreiche technische Datenbanken von den meisten Anti-Malware-Firmen: z.B. bieten Microsoft[12] und Symantec[13] derartige Informationen an, die Firma Trend Micro die „Virus Encyclopedia“[14]. Die vorliegende Arbeit konzentriert sich auf frei verfügbare Berichte über Malware bzw. IT-Sicherheits-Bedrohungen und geht nicht auf technische Sachverhalte ein.

2 Definitionen

Das Wort „Malware“ ist eine Kurzform von Malicious Software, als Übersetzung wird in der deutschen Fassung von Wikipedia das Wort „Schadprogramm“ verwendet. Die Definition lautet:

---

[11] Siehe z.B. http://futurezone.at/netzpolitik/1214-weihnachtseinkaeufe-im-netz-schaden-firmen.php, http://derstandard.at/1293369927261/Europol-750-Mrd-Euro-Schaden-pro-Jahr-weltweit-durch-Cybercrime, www.economist.com/node/17730556: New twists in the story of a mysterious and sophisticated cyber-weapon, abgefragt am 14.6.2011.

[12] http://www.microsoft.com/security/portal/, abgefragt am 4.6.2011.

[13] http://us.norton.com/security_response/index.jsp, abgefragt am 4.6.2011.

[14] http://about-threats.trendmicro.com/threatencyclopedia.aspx?language=us&tab=malware, abgefragt am 4.6.2011.

- „Als Schadprogramm oder Malware … bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und ggf. schädliche Funktionen auszuführen. … Malware wird von Fachleuten der Computersicherheitsbranche als Über- oder Sammelbegriff verwendet, um die große Bandbreite an feindseliger, intrusiver und/oder unerwünschter Software oder Programmen zu beschreiben.“[15]

Fehlerhafte Programme zählen nicht zur Malware. Allerdings ist die Abgrenzung dessen, was als Malware einzustufen ist, nicht immer eindeutig. Ein Spyware-Programm, das das Surf-Verhalten des Nutzers aufzeichnet, kann als Beispiel dienen. Sofern dieses Programm ohne Wissen und Einverständnis des Betroffenen eingesetzt wird, kann es als Malware eingestuft werden. Dies ist allerdings nicht der Fall, wenn der Nutzer mit dem Einsatz einverstanden ist oder dies sogar wünscht, um sich bei seinen Recherchen oder sonstigen Aktivitäten im Internet besser unterstützen zu lassen. Wikipedia nennt folgende Beispiele:

- “There is a group of software (Alexa toolbar, Google toolbar, Eclipse data usage collector, etc.) that send data to a central server about which pages have been visited or which features of the software have been used.”[16]

Wie schwierig die Abgrenzung zu erwünschter Software sein kann, zeigt das Beispiel eines Programms, das ein Backup der Daten eines Computers erzeugt: Wird es vom Nutzer der Daten aus Sicherheitsgründen ausgeführt, ist es ein nützliches Programm, wird es von einem „Hacker“, der die Daten absaugt, eingesetzt, ist es Malware. Die Firma McAfee bezeichnet daher gewisse Klassen von Malware als „potentially unwanted programs“[17] (PUP).

Der Empfehlung des NIST (National Institute of Standards and Technology) „Guide to Malware Incident Prevention and Handling“ SP 800-83 ([11], S. C2) kann folgende Definition entnommen werden:

- “Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.”

Nach wie vor wird im allgemeinen Sprachgebrauch der Terminus „Virus“ gleichbedeutend mit Malware verwendet, obwohl Virus eine selbstreproduzierende Malware bezeichnet und daher eine Teilkategorie von Malware ist. Sogar der „Digital Agenda Scoreboard 2011“ der EU [6] verwendet Virus im Sinne von Malware. In den diversen Publikationen über Malware werden

15 http://de.wikipedia.org/wiki/Malware, abgefragt am 4.6.2011.

16 http://en.wikipedia.org/wiki/Malware, abgefragt am 7.6.2011

17 www.mcafee.com/us/resources/white-papers/wp-potentially-unwanted-programs-spyware-adware.pdf, abgefragt am 7.6.2011

Klassifizierungen vorgenommen, die u.a. zwischen Viren, Würmern, Trojanern (trojanischen Pferden), Angriffstools und Phishing unterscheiden (siehe z.B. [11]). Diese Kategorisierungen werden allerdings je nach Organisation sehr unterschiedlich gebraucht, und da Malware mittlerweile multifunktional aufgebaut ist, d.h. die Charakteristika von mehreren Kategorien aufweisen kann, sind sie auch nicht zielführend. Dies umso mehr, als einige Malware-Programme so aufgebaut sind, dass Funktionalitäten aus dem Internet nachgeladen werden, die die Charakteristika der Malware verändern.

Abgesehen von der schwierigen Definition ist schon die Bezeichnung (Nomenklatur) von Malware eine komplexe Angelegenheit. Malware wird typischerweise von Anti-Malware-Firmen oder IT-Sicherheits-Firmen gefunden. Falls es sich um eine Malware mit einem hohen Schadenspotential handelt, werden möglichst rasch Gegenmaßnahmen ergriffen und die Namensgebung steht dann nicht im Vordergrund.

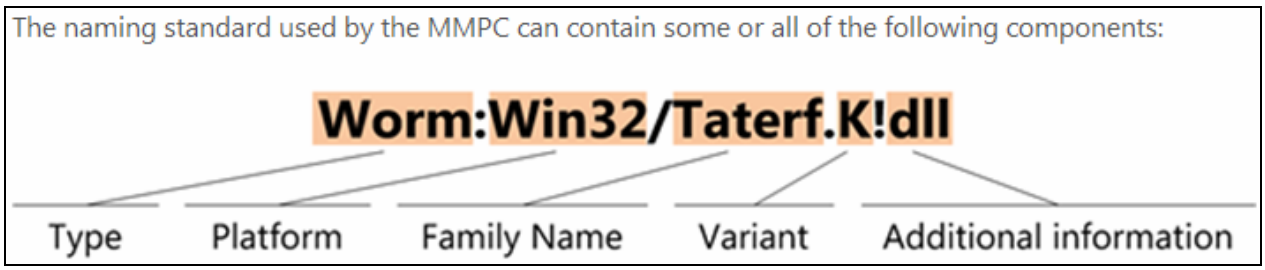
3 Malware Identifikation

Von den IT-Sicherheitsfirmen werden unterschiedliche Malware Identifikationen bzw. Bezeichnungen verwendet. Sie stützen sich auf das Namens-Schema der Computer Anti-virus Researcher Organisation (CARO: www.caro.org) aus dem Jahr 1991, das 2002 aktualisiert wurde. Dieses Schema geht davon aus, dass es nicht möglich ist, einheitliche Namen für Malware zu verwenden, da jede Firma ihre eigene Benennung vornimmt. Das Ziel sei allerdings, standardisiert aufgebaute Namen zu erhalten. Ein Malwarename setzt sich laut CARO aus folgenden Teilen zusammen:

- Name der Malware Familie
- Malwaretyp (z.B.: ‘virus’, ‘trojan’, ‘dropper’)
- Plattform (z.B. OSX für Macintosh OS X, W64 für 64 Bit Windows, XM für Excel Makro)
- Gruppenname
- Variante
- Spezifischer Kommentar der Firma

Microsoft verwendet folgende Variante des Schemas[18]:

[18] Siehe www.microsoft.com/security/portal/Shared/MalwareNaming.aspx, abgefragt am 4.6.2011



Symantec setzt eine kürzere Variante, bestehend aus Präfix, Name und Suffix ein[19].

Es bleibt allerdings das Problem bestehen, dass ein und dieselbe Malware von unterschiedlichen Firmen unterschiedliche Namen erhalten kann. Ein Beispiel dafür ist die Malware conficker[20], die von den Firmen Sophos, CA, Panda mit diesem Namen bezeichnet wurde, bei Symantec den Namen Downadup erhielt und bei Kaspersky Kido heißt.

Zum Austausch von Informationen über Viren wurde die Wildlist Organisation gegründet[21], die einen Überblick über Viren „in the wild“ (d.h. auch tatsächlich vorkommend) bietet und an die alle namhaften Anti-Malware-Firmen Malware-Samples melden. Diese monatlich veröffentlichte Liste enthält jeweils die Namen der Personen, die Meldungen abgegeben haben, und die Namen der gefundenen Malware[22,23].

Im Jahr 2004 wurde mit der CME (Common Malware Enumeration) Initiative ein neuer Versuch unternommen, einheitliche Malware-Namen (zumindest für „high profile threats“[24], d.h. besonders gefährliche Bedrohungen) zu vergeben. In diesem Fall wurden fortlaufende Nummern gewählt, um die Namen kurz zu halten, und die Klassifikation erfolgte gemeinsam mit den an der Initiative beteiligten Firmen.

Allerdings stellte sich im Jahr 2007 heraus, dass der CVE-Ansatz nicht mehr funktioniert, da sich der Malware-Einsatz grundlegend geändert hatte: Statt des Auftretens weniger heftiger Malware-Ausbrüche werden nun viele gezielte Malware-Produkte mit geringer Ausbreitung eingesetzt.

Die Anstrengungen wurden daher in der „Malware Working Group“ gemeinsam von DHS (Department of Homeland Security), DoD (Department of Defense) und NIST (National Institute of Standards and Technology) fortgesetzt. Man konzentriert sich darauf, Standards für die Beschreibung und Übermittlung von Informationen über Malware in einer eigenen Sprache zu

---

[19] Siehe http://www.symantec.com/security_response/virusnaming.jsp, abgefragt am 4.6.2011

[20] Siehe http://en.wikipedia.org/wiki/Conficker, abgefragt am 4.6.2011

[21] Siehe www.wildlist.org, abgefragt am 8.6.2011

[22] www.fortiguard.com/antivirus/wildlist.html, abgefragt am 8.6.2011

[23] http://www.viruslist.com/de/glossary?glossid=188809128, abgefragt am 8.6.2011

[24] Siehe www.malwarecity.com/blog/virus-naming-the-whos-who-dilemma-2-782.html, abgefragt am 4.6.2011

entwickeln[25]. Dabei werden unter anderem das Verhalten der Malware, ihre Angriffsmuster und weitere Attribute erfasst.

Parallel dazu werden gleichartige Anstrengungen im Rahmen der Arbeitsgruppe Industry Connections Security Group des IEEE (Institute of Electrical and Electronics Engineers) unternommen. Dies geschieht in der ICSG Malware Working Group[26] mit dem Ziel, intelligentere Mittel zum Informationsaustausch über Malware zu entwickeln, damit die Computer-Sicherheits-Industrie effektiver arbeiten kann. Dafür liegt derzeit der Entwurf für ein XML-Schema vor[27].

4 Kategorisierungsansätze

Eine erste Möglichkeit der Kategorisierung des Wissens über Malware bietet sich an, wenn man die unterschiedlichen Interessenslagen der publizierenden Organisation bei der Sammlung von Informationen über Malware in Betracht zieht.

Folgende Kategorisierungsansätze sollen hier beschrieben werden:

- *Publizierende Organisation*: Welche Organisation hat den Bericht veröffentlicht?
- *Zielgruppe*: Für wen ist dieser Bericht gedacht/konzipiert?
- *Methodologie*: Welche Methodologie wurde angewendet?
- *Plattform*: Auf welcher System-Plattform agiert die Malware?
- *Themenbereich*: Welche Themen werden behandelt?
- *Auswirkungen*: Welche Auswirkungen kann die Malware haben?

4.1 Kategorisierung nach publizierender Organisation

IT-Sicherheitsfirmen sind sehr aktiv bei der Publikation von Berichten. Als Beispiele können

Arbor Networks [3], Kaspersky[28], McAfee[29], PandaLabs [13], Symantec[30], MessageLabs Intelligence, G-Data genannt werden.

25 http://maec.mitre.org/index.html, abgefragt am 8.6.2011

26 http://standards.ieee.org/develop/indconn/icsg/malware.html, abgefragt am 8.6.2011.

27 http://grouper.ieee.org/groups/malware/malwg/Schema1.1/, abgefragt am 8.6.2011.

28 www.viruslist.com/de/analysis?pubid=200883738, abgefragt am 14.6.2011.

29 www.mcafee.com/de/resources/reports/rp-quarterly-threat-q1-2011.pdf, abgefragt am 14.6.2011.

30 www.symantec.com/business/threatreport/index.jsp, abgefragt am 14.6.2011.

Aber auch Hardware- und Software-Hersteller wie Microsoft, IBM (durch X-Force) oder CISCO (durch ScanSafe) stellen umfangreiches Datenmaterial zur Verfügung. Dienstleister wie Akamai oder die Malware Research Group[31] sowie Beraterfirmen (Capgemini, PWC) sind ebenfalls präsent. Weiters gibt es Berichte von Computer Emergency Response Teams CERTs (CERT-FI[32], GovCert.NL [8], CERT.at und GovCERT.at[33]) und von speziellen, zum Teil gemeinnützigen, Organisationen wie APWG (Anti Phishing Working Group), ShadowServer Foundation oder OWASP (Open Web Application Security Project) wird ebenfalls Datenmaterial zur Verfügung gestellt.

Im Rahmen der Verfolgung von Cyber-Crime Aktivitäten steigt das Interesse der Strafverfolgungsbehörden an Malware. Da Computer-Kriminalität meist länderübergreifend erfolgt, müssen Strafverfolgungsbehörden mehrerer Staaten zusammenarbeiten, was neue Ansätze erfordert. Berichte dazu gibt es von Europol [7].

Weiters werden Informationen über Malware auch von internationalen Organisationen wie der OECD (Organisation für wirtschaftliche Entwicklung und Zusammenarbeit) [12], veröffentlicht. Die Europäische Kommission hat im Rahmen der „Digitalen Agenda für Europa“, einer der 7 Leitinitiativen der Strategie Europa 2020, ein Scoreboard [6] erstellt, das ebenfalls Informationen über Malware enthält. Auch staatliche Organisationen wie das BSI (Bundesamt für Sicherheit in der Informationstechnik in Deutschland) [5] oder das US-Amerikanischen Normungsinstitut NIST [11] erheben und publizieren Daten und Informationen über Malware.

4.2 Kategorisierung nach Zielgruppe

Die untersuchten Berichte sind zum Teil an bestimmte Adressaten gerichtet, andere geben keine explizite Zielgruppe an.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) richtet seine Quartalsberichte [5] an „IT-Sicherheitsbeauftragte, Verantwortliche für IT-Systeme sowie interessierte Bürgerinnen und Bürger“, um einen Überblick über die Lage der Internetsicherheit zu geben. Dabei wird auch erläutert, wie einzelne aktuelle Malware-Produkte funktionieren und welchen Zweck ihr Einsatz hat. Unter anderem wird der Angriff auf den Emissionshandel der EU, bei dem bis zu zwei Millionen Zertifikate im Wert von rund 30 Millionen Euro gestohlen wurden, beschrieben.

Der Bericht „2010 National Cyber Crime and Digital Safety Trend Report“ des niederländischen Government CERT [8] richtet sich an politische Entscheidungsträger,

[31] http://malwareresearchgroup.com/, abgefragt am 13.6.2011.

[32] www.cert.fi/attachments/tietoturvakatsaukset/5waQucyMp/CERT-FI_annual_report_2010.pdf, abgefragt am 14.6.2011.

[33] www.digitales.oesterreich.gv.at/site/6828/default.aspx, abgefragt am 14.6.2011.

die Verwaltung und Betriebe im Bereich der kritischen Infrastrukturen sowie IT-Sicherheits-Fachleute. Der Bericht soll als Grundlage für strategische Entscheidungen dienen.

Die Firma Sophos gibt alle Internet-Nutzer als Zielgruppe für ihren Bericht „Security threat report 2011“ [16] an und untersucht die Frage, welches Risiko der Nutzer eingeht. Zitat:

- “Malware attacks can strike at anytime and from anywhere. Weak passwords, mobile devices and social networks, everyday software, removable media, operating systems and web all pose risk.”

Der „Worldwide Infrastructure Security Report 2010“ von ArborNetworks wendet sich ebenfalls an eine spezielle Zielgruppe, nämlich Internet Service Provider.

Bei einigen Berichten ist allerdings keine explizite Zielgruppe ersichtlich (z.B. der Jahresbericht des Cert.fi[34]); Sie können als allgemeine Lageberichte eingestuft werden.

Im Rahmen des bereits erwähnten Scoreboard der „Digitalen Agenda“ [6] werden Daten erhoben, die den Zielerreichungsgrad von „Every European Digital“ (Ausspruch von EU-Kommissarin Kroes[35]) messen und dabei auf die Fragen der Sicherheitsbedenken von Bevölkerung und Firmen, die tatsächlich entstandenen Schäden und die ergriffenen Schutzmaßnahmen eingehen.

4.3 Kategorisierung nach angewendeter Methode

In den untersuchten Berichten werden sehr unterschiedliche Methoden der Ermittlung von Informationen über Malware angewendet, aber nur teilweise offen gelegt. Generell werden Daten veröffentlicht, die aus Umfragen stammen, bzw. Daten, die aufgrund der Tätigkeit der berichtenden Organisation anfallen (u.a. Analyse von Mailverkehr, von Webabfragen und von Malwaresamples) und ausgewertet werden. Teilweise werden auch Ergebnisse und Berichte anderer Organisationen und sonstige Veröffentlichungen mit einbezogen.

Die Europäische Kommission gibt in ihrem Bericht „Digital Agenda Scoreboard 2011“ ([6], p.20] in einem eigenen Kapitel detaillierte Angaben über die eingesetzte Methode. Es handelt sich um eine repräsentative Umfrage unter Internet-Nutzern.

Der Bericht von McAfee und CSIS „In The Dark“ [4] stützt sich auf die Befragung von 200 Führungskräften in Betrieben aus dem Bereich der kritischen Stromversorgungs-Infrastruktur aus 14 Ländern.

---

[34] www.cert.fi/attachments/tietoturvakatsaukset/5waQucyMp/CERT-FI_annual_report_2010.pd, abgefragt am 14.6.2011.

[35] http://blogs.ec.europa.eu/neelie-kroes/every-european-digital-means-exactly-that/, abgefragt am 14.6.2011.

Arbor Networks verwertet bei seinem Bericht „Worldwide Infrastructure Security Report, 2010 Report“ [3] Daten einer Umfrage bei Internet Service Providern. Es wurden Fragebögen mit 113 offenen und Multiple-Choice Fragen von 111 Organisationen beantwortet.

Der „McAfee Threat Report“ [Af3] nützt ein Netz von Millionen von Sensoren weltweit sowie den cloudbasierten Dienst McAfee Global Threat Intelligence, 350 multidisziplinäre Forscher, die in 30 Ländern für McAfee Labs arbeiten, um Informationen über Bedrohungsvektoren zu sammeln und auszuwerten. Ebenfalls auf umfangreichem Datenmaterial (Reports von mehr als 130 Millionen Systemen im Internet, Daten von 240.000 Netzwerksensoren in über 200 Ländern, Überwachung von mehr als 35.000 Schwachstellen, die über 80.000 Technologien von über 11.000 Anbietern betreffen) beruht der Bericht von Symantec[36].

Der Bericht der Firma Sophos [16] stützt sich auf die von der Firma analysierten Malware-Samples (2010: 95.000 pro Tag, fast doppelt soviel wie 2009) und gibt einen Überblick über die von der Firma diagnostizierten neuen „Trends“ (z.B. Fake Antiviren-Software, Search Engine Optimization Attack). Weiters gibt es punktuelle Auswertungen von SPAM, der in Sozialen Netzwerken verteilt wird, sowie Angaben über Phishing und Malware Trends (Wachstumsraten in Prozent).

Der Malware-Report der Firma Kaspersky, 1. Quartal 2011[37], basiert auf Auswertungen von statistischen Daten von Kaspersky Web-Anti-Virus, das Anwender vor dem Download schädlicher Codes von infizierten Webseiten schützt. Das können Seiten sein, die von Cyberkriminellen speziell erstellt wurden, Web-Ressourcen, deren Inhalt beispielsweise bei Foren von Anwendern gestaltet wird, oder gehackte Webseiten. Allerdings handelt es sich lediglich um Daten, deren Veröffentlichung die Kunden zugestimmt haben.

Die Firma Akamai [1] verwendet für ihre Auswertungen, die sich auf „Attack Traffic“ konzentrieren, jene Daten, die sie durch ihre global verteilten Server-Netzwerke erhält. Dieser „Attack Traffic“ wird in Prozent des Gesamt-Internet-Traffics angegeben. In einer länderspezifischen Auswertung wird dieser Anteil für die USA z.B. mit 7,3%, für Österreich mit 0,2% angegeben.

Für die Berichterstattung wird auch die Dokumentation von einzelnen spektakulären Zwischenfällen herangezogen. Dies ist im Bericht „Night Dragon“ von McAfee [10] der Fall, der einen Angriff im Bereich der Energieversorgung beschreibt.

[36] www.symantec.com/business/threatreport/index.jsp, abgefragt am 14.6.2011.

[37] www.viruslist.com/de/analysis?pubid=200883738, abgefragt am 14.6.2011.

Eine interessante Methode setzt die Firma Malware Research Group ein. Es werden sogenannte „Flash Test Results“ ermittelt[38], wobei getestet wird, ob die Anti-Malware Produkte von IT-Sicherheitsfirmen (u.a. Avira, Kaspersky, McAfee) kürzlich bekannt gewordene Malware (jünger als eine Woche) erkennen und die Resultate verglichen.

4.4 Kategorisierung nach Träger-System

Die Entwicklung von Malware zeigt, dass laufend neue Träger-Systeme für Malware und angegriffene Systeme in Form von Hardware, Software, Software-Produkten, Software-gesteuerten Geräten erschlossen werden. Malware wird jeweils auf einem bestimmten System wirksam. Das können Betriebssystem-Plattformen auf PCs oder Notebooks sein (Microsoft Windows, Apple Mac OS/X), weiters Betriebssysteme auf mobilen Geräten wie Smartphones (Android, iOS, Windows Mobile, Symbian), aber auch Software-Plattformen, wie z.B. Java, Adobe Air, .NET Framework eignen sich als Trägersysteme, ebenso wie sonstige Software-Produkte. Derzeit ist PDF (Portable Dokument Format) von Adobe ein wesentlicher Träger für Malware, aber auch Microsoft-Office Produkte werden seit geraumer Zeit als Malwareträger genutzt. Eine interessante Gegenüberstellung der Anfälligkeit dieser beiden Produkte findet sich in dem Bericht „The Rise of PDF Malware“ von Symantec [14], aus dem hervorgeht, dass im Jahr 2009 zwar mehr Schwachstellen in Office-Produkten als in PDF bekannt waren, PDFs aber für wesentlich mehr Angriffe genutzt wurden.

Weitere sehr intensiv genutzte Träger-Systeme sind seit einigen Jahren mit Malware infizierte Webangebote (Siehe BSI-Lagebericht IT-Sicherheit 2009[39], S. 69 driveby-downloads).

Seit der Entdeckung der Malware Stuxnet[40] ist erwiesen, dass auch industrielle Steuerungsanlagen bzw. SCADA-Systeme als Träger-Systeme für Malware genützt werden. Da derartige Systeme bei der Steuerung von kritischen Infrastrukturen, wie z.B. Strom- bzw. Gasversorgung, eingesetzt werden, können durch Einsatz von Malware auch wichtige Basisdienste der Gesellschaft gestört werden.

[38] http://malwareresearchgroup.com/malware-tests/flash-test-results/, abgefragt am 13.6.2011.

[39] https://www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html, abgefragt am 14.6.2011.

[40] http://en.wikipedia.org/wiki/Stuxnet, abgefragt am 14.6.2011.

4.5 Kategorisierung nach Themenbereich/Art der untersuchten Malware

In einigen Berichten werden sowohl Anzahl an bekannter als auch Zuwachsraten an neuer Malware untersucht und auch eine Einteilung in einzelne Untergruppen durchgeführt. Aus dem Bericht „THE CYBER-CRIME BLACK MARKET: UNCOVERED“ [13] geht hervor, dass PandaLabs im Jahr 2008 14 Mio. Malware-Familien erfasst hatten, im Jahr 2010 wuchs diese Zahl auf 60 Mio. Exemplare an, wobei Trojaner mit 70% am häufigsten auftraten. Der Messagelabs Intelligence (MLI) Report von April 2011[41] untersucht den Anteil der Malware in E-Mails und kommt auf einen Wert von 1:284, der seit 2009 unverändert geblieben ist.

Ein anderer Zugang ist die Messung der abgewehrten Attacken, so wie dies der Malware-Report von Kaspersky Lab, erstes Quartal 2011[42] ergab, der 250 Mio. Angriffe im Untersuchungszeitraum feststellte. Auf 77 gezielte Mail-Attacken täglich im Jahr 2010 (48 in 2009) kommt der MLI Report von April 2011.

SPAM ist ein weiteres Untersuchungsgebiet, bei dem unterschiedliches Zahlenmaterial erhoben wird. Der „McAfee Threat-Report: Erstes Quartal 2011“[43] stellt eine deutliche Abnahme von SPAM fest, und zwar von ca. 5 Billiarden SPAM Mails im Juli 2010 auf ca. 1,5 Billiarden im März 2011. Vergleicht man dieses Resultat mit dem MLI Report von April 2011 (siehe Fußnote 31), so wird in diesem Bericht von 66 Mrd. Mails pro Tag im März ausgegangen (entspricht ca. 2 Billionen Mails pro Monat) und davon ca. 1,5 Billionen SPAM pro Monat. Ein Bericht der Firma Commtouch „Internet Threats Trend Report April 2011“[44] sieht eine Abnahme von 165 Mrd. SPAM/Tag (4,9 Billionen/Monat, Februar 2010) auf 120 (3,6 Billionen/Monat, Oktober 2010). Die gemeinsame Aussage ist, dass die Anzahl der SPAM-Mails abnimmt. MLI (siehe Fußnote 31) analysiert SPAM-Aufkommen noch weiter im Detail und berichtet von einer „average global spamrate“ von 89,1% im Jahr 2010, das ist um 1,4% mehr als 2009. 88,2% der SPAMs-Mails wurden über Botnetze verteilt.

Die Firma Sophos untersucht in ihrem Bericht [16] den Prozentsatz an SPAM, Phishing und Malware in Sozialen Netzen, wobei die Resultate auf einer Umfrage beruhen. Dabei geben 67% der Befragten an, SPAM über soziale Netzwerke erhalten zu haben, 43% Phishing-Angriffe und 40% Malware. Der bereits zitierte Bericht von Kaspersky beziffert das Aufkommen an neuen Signaturen für Malware für mobile Geräte im Jahr 2010 mit 500 und rechnet mit einer jährlichen Verdoppelung dieses Wertes.

---

[41] Siehe www.messagelabs.com/resources/mlireports.aspx, p.19, abgefragt am 14.6.2011.

[42] www.viruslist.com/de/analysis?pubid=200883738, abgefragt am 14.6.2011.

[43] www.mcafee.com/de/resources/reports/rp-quarterly-threat-q1-2011.pdf, abgefragt am 14.6.2011.

[44] www.commtouch.com/download/1996, abgefragt am 14.6.2011.

Als Themenbereiche kommen sehr unterschiedliche Fragestellungen vor. Der Bericht der APWG Anti Phishing Working Group)[45] interessiert sich z.B. für Malware nur insofern, als es ein Werkzeug zum Phishen (Passwort-Diebstahl) ist.

Weitere Auswertungen betreffen Aussagen darüber, in welchen Ländern die meisten kompromittierten seriösen Webseiten lokalisiert sind ([16], S.37). Bei weitem die meisten treten in den USA auf (39%), gefolgt von Frankreich (10%), Russland und Deutschland.

Besondere Aufmerksamkeit finden Botnetze, da sie u.a. zu den Hauptmechanismen gehören, über die Malware verteilt wird. Diesbezügliche Zahlenangaben finden sich bei der Shadowserver Foundation[46], die die Anzahl der aktiven Command and Control Server (die „Steuereinheiten" der Botnetze) misst (derzeit ca. 5.000). Die Firma Sophos ([16], S.37) berichtet von 30.000 verseuchten Webadressen täglich, von denen 70% seriöse Webseiten sind.

Weitere interessante Themen sind die "patch rates", d.h. die Reaktionsgeschwindigkeit der Herstellerfirmen bei der Reparatur von Schwachstellen ihrer Programme. Der Bericht von IBM X-Force[47] liefert hier interessantes Zahlenmaterial über veröffentlichte Schwachstellen, für die noch keine Patches zur Verfügung standen. Zieht man alle Hersteller heran, so sind für 55% keine Reparaturen verfügbar, während dieser Wert für Microsoft bei 23% liegt, für Apple bei 12%.

Zunehmend widmen sich Berichte dem Thema Malware und kritische Informations-Infrastrukturen. (siehe Berichte von McAfee ([4], [10]), National Institute of Standards and Technology (NIST)[48]). Es handelt sich um ein neues Anwendungsfeld für Anti-Malware-Einsatz in äußerst sensiblen Bereichen.

Besonders schwierig zu erkennen sind RAT-Systeme (remote administration tools), die es einem Angreifer erlauben, ein System vollständig zu steuern. Derartige RAT-Systeme können nur dann identifiziert werden, wenn ein gesamtes RAT-Toolkit gefunden wird und untersucht werden kann (Siehe [10], S. 7).

4.6 Kategorisierung nach Auswirkungen

Die Auswirkungen von Malware reichen von der Infektionen einzelner Computer die praktisch keine Auswirkungen haben, bis zur Lahmlegung von Unternehmen bzw. Störungen bei kritischen Infrastrukturen eines Landes. Im Folgenden einige Beispiele:

---

[45] www.antiphishing.org/, abgefragt am 14.6.2011.

[46] www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts/, abgefragt am 10.6.2011.

[47] Siehe www-935.ibm.com/services/us/iss/xforce/trendreports/ S.20, abgefragt am 10.6.2011.

[48] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, abgefragt am 10.6.2011.

- Laut einem Bericht des Govcert.NL [8] sind 0,5 bis 5% aller Computer mit Malware verseucht, wobei es sich hauptsächlich um die Rechner von Heimanwendern und KMUs handelt.
- Eine der Auswirkungen von über Malware verteiltem SPAMs wird in einem Artikel von BBC News[49] erläutert: Schätzungsweise 36 Millionen US-Amerikaner erwerben Medikamente von nicht zugelassenen Online-Verkäufern.
- Europol bewertet im iOcta-Bericht ([7], S. 5) den finanziellen Schaden, der durch Cyber-Kriminalität verursacht wurde, und zitiert dabei eine Schätzung von 775 Mrd. Euro weltweit (Zitat einer Aussage von McAfee[50]).
- Die Europäische Kommission geht in ihren Analysen zur Digitalen Agenda von negativen Auswirkungen von Malware auf die wirtschaftliche Entwicklung insoweit aus, als Bürger und Wirtschaft aufgrund von Malware digitalen Dienstleistungen weniger vertrauen, wodurch die Akzeptanz dieser Dienste daher herabgesetzt ist.

5 Prinzipielle Überlegungen

In einem Bericht an die Parlamentarische Versammlung der NATO mit dem Titel „Information and National Security“ ([9], Kap. IV) wird Malware als das wesentliche Instrument für Cyber-Angriffe genannt. Es wird auch darauf hingewiesen, dass Malware gekauft oder auch kostenlos aus dem Internet bezogen werden kann. Malware stellt daher eine massive Bedrohung für die nationale Sicherheit von Staaten dar. Wie Stuxnet gezeigt hat, können durch Malware auch die kritischen Infrastrukturen eines Landes angegriffen und in ihrer Funktionsfähigkeit gestört werden [2].

Malware wird zunehmend auch für kriminelle Aktivitäten benutzt, da die Strafverfolgung an nationale Grenzen gebunden ist, die Gesetzeslage zum Teil den technischen Möglichkeiten hinterher hinkt und für die Verfolgung von Cyber-Kriminalität viel aktuelles Know-how nötig ist. Diese Umstände tragen dazu bei, dass Cyber-Kriminalität stark zunimmt.

Ebenso kann Malware dazu eingesetzt werden, Behörden und Firmen in ihrer Tätigkeit zu behindern bzw. zu schädigen. Auf der Ebene der Heimanwender schließlich können diese entweder selbst geschädigt oder ihre Computer benutzt werden, um Straftaten zu begehen.

Malware stellt daher eine massive Gefährdung dar. Allerdings ist die Öffentlichkeit offenbar bereit, mit diesem nicht unerheblichen Risiko zu leben.

---

[49] www.bbc.co.uk/news/technology-12017185?print=true, abgefragt am 10.6.2011.

[50] http://blogs.mcafee.com/corporate/ceo-perspectives/unsecured-economies-%E2%80%93-a-trillion-dollar-headwind, abgefragt am 10.6.2011.

Dies geht aus dem Bericht „National Cyber Crime and Digital Safety Trend Report“ des niederländischen GovCert hervor ([CERT.nl 1], p.39 ff.), der darauf hinweist, dass sowohl Heimanwender als auch Firmen ausreichend Vertrauen in ihre IT-Sicherheitsmaßnahmen haben, um Computer und Internet weiterhin intensiv zu nutzen (Zitat: „The risk perception of civilians and companies does not match the actual risks.“). Das ist allerdings vor dem Hintergrund zu sehen, dass sowohl Firmen als auch Heimanwender zunehmend abhängig von Informations- und Kommunikationstechnologie sind.
Aus dieser Perspektive stellt sich die Frage, wie mit den Malware-Bedrohungen umgegangen werden soll bzw. welche Player aktiv werden sollen. Ein Hintergrundbericht der OECD aus dem Jahr 2008 [12] setzt sich mit den Anreizen auseinander, die die einzelnen Player haben, die Sicherheit zu erhöhen. Als Player werden von der OECD Internet Service Provider (ISP), Software Anbieter, Hardware Erzeuger, e-commerce Firmen, Registrare, Heimanwender, Regierungen und Verwaltungen gesehen. Der Bericht der OECD ortet ein prinzipielles Problem, nämlich dass die Kosten für Schäden häufig nicht von den Verursachern getragen werden. Zum Beispiel kann Software, die nicht ausreichend sicher ist und Schwachstellen hat, bei den Heimanwendern zu Problemen führen, da sie Ziel von kriminellen Cyber-Attacken werden können, allfällige Schäden aber von dem Software-Hersteller nicht refundiert werden. Eine ähnliche Problemstellung gibt es bei ISPs, die nur begrenzt Anreize haben, gegen Malware bzw. Angriffe, die über ihre Server laufen, einzugreifen.

Europol setzt sich mittlerweile intensiv mit Cyber-Kriminalität auseinander und fungiert als Kommunikationsplattform der nationalen Strafverfolgungsbehörden in der Europäischen Union. Der iOtca-Bericht [7] aus dem Jahr 2011 weist darauf hin, dass energische Anstrengungen nötig sein werden, um die Cyber-Kriminalität zu bekämpfen.

Ein kürzlich erschienener Bericht im Zuge des OECD Projekts “Future Global Shocks” mit dem Titel “Reducing Systemic Cybersecurity Risk” ([15], S. 42) weist auf die Schwierigkeiten bei der Lagebeurteilung hin:

- “One of the difficulties in promoting a sober public assessment of cybersecurity threats is the plethora of articles and news-features which extrapolate speculatively from the uncovering of program or operating system flaws, or from the news that an item of malware uses a hitherto unknown technique and has been found in the wild.”

Zusammenfassend lässt sich sagen, dass die Verbreitung von Malware massiv zunimmt, ein hohes Schadenspotential aufweist, die Gegenmaßnahmen aber nach wie vor sehr fragmentiert sind.

6 Schlussfolgerungen

Malware ist omnipräsent und bietet die Möglichkeit, IT-gesteuerte Systeme zu knacken und für andere Zwecke als ursprünglich vorgesehen zu nutzen. Der allgemeine Trend geht dahin, Systeme zu entwickeln und zu nutzen, die „intelligent“ sind (siehe z.B. die Initiative Europa 2020, Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum[51]), um z.B. den Energieverbrauch zu verringern, Autofahrer besser zu unterstützen (Stauwarnung, Unfallwarnung), die Stromversorgung ökologischer zu gestalten („smart grids“), Online-Gesundheitsdienste zu fördern. Da IT-Sicherheit allerdings beim Aufbau derartiger Systeme nicht immer von vornherein berücksichtigt wird, nimmt die Bedrohung durch Malware weiter zu.

Bei der Beurteilung der Lage sollte man auch bedenken, dass laut einer Studie der OECD ([15], S.7) Malware von sehr unterschiedlichen Gruppen mit sehr unterschiedlichen Zielsetzungen erzeugt und eingesetzt wird:

- “There are many different actors and with varying motivations in the cybersecurity domain. Analysis and remedies which work against one type may not be effective against others. Among such actors are: criminals, recreational hackers, hacktivists, ideologues, terrorists, and operatives of nation states.”

Mittlerweile hat sich auch die Art und Weise, wie Malware eingesetzt wird, grundlegend verändert. Wie oben erwähnt, ist man von einer Massenverteilung zu gezielten Angriffen übergegangen, die nur auf wenige Ziele verteilt werden. Dadurch konnte die Sichtbarkeit der Angriffe verringert werden, und damit erhöht sich die Chance, nicht erkannt zu werden. Wie aus einer Präsentation bei der Industry Connections Security Group der IEEE[52] hervorgeht, erfolgt die Behandlung von Malware-Bedrohungen durch die IT-Sicherheits-Firmen jeweils im Rahmen ihrer eigenen Möglichkeiten und mit relativ wenig Kooperation mit anderen Akteuren. Im Gegensatz dazu hat es die Untergrund-Wirtschaft verstanden, Massenproduktionsvorteile zu lukrieren und sich Zugang zu Spezial-Tools und –Diensten zu verschaffen.

Dies spricht sehr klar dafür, dass für die Eindämmung und Bekämpfung von Malware intensive Kooperationen zwischen den einzelnen Akteuren notwendig sind. Allerdings behindern unterschiedliche Interessenslagen und mangelnde Kooperation die Intensivierung einer abgestimmten internationalen Vorgangsweise.

---

[51] http://ec.europa.eu/eu2020/pdf/COMPLET%20%20DE%20SG-2010-80021-06-00-DE-TRA-00.pdf, abgefragt am 15.6.2011

[52] http://standards.ieee.org/develop/indconn/icsg/, abgefragt am 15.6.2011

Neben den bereits genannten Anzeichen für eine Verstärkung der Kooperation (Caro, Wildlist, IEEE) kann man allerdings konstatieren dass z.B. mittlerweile auch CERTs (Computer Emergency Respose Teams) aus dem Bereich der Strafverfolgung Mitglieder bei FIRST, dem internationalen Dachverband der CERTs sind, oder auch, dass Interpol Mitglied im GAC (Governmental Advisory Committee) der ICANN werden will. Damit wird das Verständnis der Player für die Handlungsmöglichkeiten sämtlicher Beteiligten verstärkt.

Allerdings bleiben nach wie vor Defizite bei der Klassifizierung von Malware, aber auch bei der Meldung von Zwischenfällen bestehen, da eine Vielzahl an aufeinander nicht abgestimmten Meldestellen existiert. Weiters mangelt es an zuverlässigen und vergleichbaren statistischen Daten über Malware, weil die derzeit verfügbaren Zahlenmaterialien unvergleichbar und unvollständig sind.

Literatur

[1] AKAMAI, 2011, The State of the Internet, 4th Quarter, 2010 Report, www.akamai.com/stateoftheinternet/, abgefragt am 15.6.2011.

[2] ALBRIGHT, D., BRANNAN, P. WALROND, C., 2011, ISIS (Institute for Science and International Security), Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, www.isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/, abgefragt am 15.6.2011.

[3] ARBOR NETWORKS, 2010, Worldwide Infrastructure Security Report, 2010 Report, www.arbornetworks.com, abgefragt am 13.6.2011.

[4] BAKER, S.; FILIPIAK, N.; TIMLIN, K., 2011, In the Dark: Crucial Industries Confront Cyberattacks, www.mcafee.com/cip_report, abgefragt am 13.6.2011.

[5] BSI (Bundesamt für Sicherheit in der Informationstechnik) Nationales IT-Lagezentrum, 2011, Lagebericht 4. Quartal 2010, https://www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html, abgefragt am 13.6.2011.

[6] EUROPÄISCHE KOMMISSION, 2011, Digital Agenda Scoreboard 2011, http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/pillar/security.pdf, abgefragt am 13.6.2011.

[7] EUROPOL, 2011, iOCTA: THREAT ASSESSMENT, INTERNET FACILITATED ORGANISED CRIME, The Hague, www.europol.europa.eu/publications/Serious_Crime_Overviews/Internet Facilitated Organised Crime iOCTA.pdf, abgefragt am 13.6.2011.

[8] GOVCERT.NL, 2011, 2010 National Cyber Crime and Digital Safety Trend Report, www.govcert.nl/english/service-provision/knowledge-and-publications/trend+reports/trend-report-2010.html, abgefragt am 13.6.2011.

[9] JOPLING, 2011, NATO Parliamentary Assembly, INFORMATION AND NATIONAL SECURITY, www.nato-pa.int/default.asp?SHORTCUT=2443, abgefragt am 15.6.2011.

[10] MCAFEE, 2011, Global Energy Cyberattacks: “Night Dragon”, www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf, abgefragt am 13.6.2011.

[11] MELL, P., KENT, K., NUSBAUM, P., 2005, National Institute of Standards and Technology (NIST), Guide to Malware Incident Prevention and Handling, http://csrc.nist.gov/publications/PubsSPs.html, abgefragt am 13.6.2011.

[12] OECD, 2008. Economics of Malware: Security Decisions, Incentives and Externalities, www.oecd.org/dataoecd/53/17/40722462.pdf/, abgefragt am 15.6.2011.

[13] PANDA SECURITY, 2011, THE CYBER-CRIME BLACK MARKET: UNCOVERED, http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf, abgefragt am 15.6.2011.

[14] SELVARAJ, K., GUTIERREZ, N., 2010, SYMANTEC, The Rise of PDF Malware, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_rise_of_pdf_malware.pdf, abgefragt am 13.6.2011.

[15] SOMMER, P., BROWN, I., 2010, Reducing Systemic Cybersecurity Risk, www.oecd.org/dataoecd/57/44/46889922.pdf, abgefragt am 15.6.2011.

[16] SOPHOS, 2011, Sophos Security Threat Report 2011, www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx, abgefragt am 13.6.2011.

VON DER SICHERHEIT IM KOLLEKTIV ZUM SCHUTZ DES INDIVIDUUMS: EIN PARADIGMENWECHSEL

Rolf von Roessing

Cyber Security ist in Forschung und Praxis in erster Linie auf Organisationen gerichtet. Cyber Crime hingegen richtet sich mehrheitlich gegen das Individuum, das auch innerhalb einer Organisation regelmäßig als Schwachstelle gilt. Diese Asymmetrie führt immer häufiger zum systemischen Versagen herkömmlicher Sicherheitskonzepte. Es wird unter Anwendung des ISACA-Sicherheitsmodells BMIS gezeigt, daß nur durch einen Paradigmenwechsel hin zu einer individuellen Cyber Security eine wirksame Antwort auf die ansteigende Cyber-Kriminalität gefunden werden kann.

1 Einführung

Cyber Security als Teil der allgemeinen Unternehmenssicherheit hat in den vergangenen Jahren, wohl auch aufgrund der wachsenden Anzahl von Sicherheitsvorfällen, erheblich an Bedeutung gewonnen. Die wachsende Durchdringung der Informationstechnik in Wirtschaft und der Privatsphäre hat gleichzeitig zu einer Unverzichtbarkeit und Unabdingbarkeit elektronischer Geschäftsprozesse und -modelle geführt; schon heute ist es beispielsweise kaum mehr möglich, Zahlungsvorgänge in papierhafter Form durchzuführen. Bedauerlichweise werden diese Entwicklungen von einem rapiden Anstieg der Kriminalität begleitet, die sich in neuen Tatbeständen und Tathergängen manifestiert.

Sowohl ausschließlich elektronische als auch IT-gestützte Geschäftsprozesse werden aus Sicht der Forschung und der Praxis überwiegend aus der Sicht der anbietenden Organisationen gesehen. Für Unternehmen, Behörden und Nationalstaaten stehen umfassende, aber auch hochspezialisierte Lösungen und Produkte zur Verfügung. Wesentlich geringere Aufmerksamkeit wird dem Individuum gewidmet; der Mensch als kleinste, aber wichtigste Einheit im Sicherheitsgeschehen wird teils als unmündiger Schutzbefohlener [1], teils als argloser Wegbereiter sicherheitsrelevanter Ereignisse gesehen. Weitgehend unkritisch unterscheidet die populäre Literatur zudem zwischen „Menschen“ im eigentlichen Sinne und „Hackern“ als Symbol für jene Personen, die durch kriminelle Handlungen auffällig werden [2]. Schlußendlich erfolgt sogar – ebenfalls ohne kritische Würdigung – eine Unterteilung der Bevölkerung in eine „Zivilgesellschaft“

und eine „Internet-Gemeinde“[3], wobei letztere nach der herrschenden politischen Meinung isoliertes Gedankengut vertritt und nicht repräsentativ für die Bevölkerungsmehrheit sein soll [4].

Diese durchaus angreifbaren soziologisch-politischen Differenzierungen in individueller Hinsicht beruhen auf einem entscheidenden Wahrnehmungsirrtum. Menschen als Einzelpersonen werden nämlich nicht durch ihr IT-Wissen und ihre (vermeintliche) Zugehörigkeit in einer von der Politik postulierten Gruppe verortet. Vielmehr ist fast jeder Mensch mehrmals täglich damit konfrontiert, auch bei moderater Nutzung des Internet und seiner Angebote Sicherheitsfragen zu bedenken. Die Politik beantwortet dieses Dilemma durch das Prinzip der wohlmeinenden Bevormundung [5]; die Wissenschaft hat nur für jene Menschen eine Antwort, die bereits *ex ante* ein weit überdurchschnittliches Wissen haben, das den Zugang zur technischen Sicherheitsliteratur überhaupt erst ermöglicht. Die Wirtschaft schließlich verhindert – bis dato [6] – durch präventive Restriktionen der IT-Nutzung die Auseinandersetzung der Menschen mit scheinbar gefahrgeneigten Technologien, Internet-Angeboten und bisweilen überhaupt mit Innovationen. Das im Unternehmen stattfindende IT-Geschehen liegt oft ein bis zwei Generationen hinter dem Stand des Marktes [7] und erzeugt so neben Frustration auch eine Scheinsicherheit durch innovationsfeindliche Selbstzufriedenheit.

Neue Formen des Cyber Crime, ebenso wie neuartige Sicherheitsvorfälle, erzeugen in der heutigen Praxis in erster Linie neue Vorschriften und Beschränkungen. Organisierte Kriminalität ist in sich die Negation ebendieser Vorschriften, und Sanktionsmöglichkeiten sind aufgrund der in Kompetenz und Budget oft eingeschränkten Strafverfolgung nicht in ausreichendem Maße gegeben. Erst in zweiter Linie werden technische Lösungen erarbeitet, die jedoch aufgrund der anschwellenden Vorschriftenlast nur langsam greifen können.

Es kommt zu einem paradoxen Ergebnis: weite Teile der Bevölkerung verharren in einem Zustand der Schutz- und Hilflosigkeit, während die Hemmschwelle für Cyber-Delikte beständig sinkt. Abgesehen von unerlaubter Selbstjustiz ist der Mensch auf den nationalstaatlichen Ordnungsrahmen zurückgeworfen, während organisierte Kriminelle resilient [8] und weit jenseits nationaler Grenzen agieren. Diese Entwicklung kann ferner dazu führen, daß die IT-Kompetenz der Menschen wie ihrer Organisationen durch Verregelung eingeschränkt wird, während außerhalb des Gesetzes handelnde Akteure höhere Kompetenz in der Tatplanung und geringeres Risiko in der Tatausübung für sich verbuchen können.

Im folgenden wird gezeigt, daß dieses Dilemma zu einer schleichenden Zersetzung des herrschenden Sicherheitsparadigmas geführt hat. Es wird ferner gezeigt, daß zukünftige Sicherheitskonzepte in erster Linie auf der Ebene des Individuums angesiedelt sein müssen, um in der Cyber Security die gewünschte Wirkung entfalten zu können. Anhand von Beispielen wird verdeutlicht, wie sehr die dem Kollektiv verpflichtete „einheitliche“ Implementierung von Sicherheit zwar die vermeintlichen Bedürfnisse hierarchisch organisierter Organisationen und

Gemeinwesen bedient, jedoch in diesem Punkt der Gegenseite – dem Cyber Crime – geradezu in die Hände spielt. Genau an dieser Stelle erweist sich ein individuelles Sicherheitsparadigma als außerordentlich nützlich, um neben dem gesellschaftlich-politischen Konsens eine personenbezogene Lösungsstrategie anzubieten. Grundlage dieser Strategie ist das Sicherheitsmodell BMIS, dessen systemische Gesamtsicht einen raschen Zugang ermöglicht. BMIS hat zudem den entscheidenden Vorteil wohldefinierter Verbindungen (Mappings) zu traditionellen Rahmenwerken in der Informationssicherheit [9].

2 Konzepte der Cyber Security

Die Sicherheit im Cyberspace folgt zum jetzigen Zeitpunkt fast ausschließlich traditionellen Sicherheitsmustern. Die Vision eines „Onward Cyber Soldiers“ [10] mag Wirklichkeit geworden sein, doch die Mittel der Absicherung sind sowohl in militärischer als auch ziviler Hinsicht noch immer an die Vorstellungswelt einer hierarchischen, definiert geregelten und jederzeit beherrschbaren informationellen Umgebung angelehnt. Im Hinblick auf Cyber Crime und Cyber Warfare gilt, daß eskalierende Angriffe und Verbrechen zu staatlichen oder organisatorischen Reaktionen führen, die von zielgerichtetem Einsatz der Technik über verschiedene Governance- und Compliance-Ansätze bis hin ins Surreal-Groteske [11] reichen, bisweilen sogar in die verträumte Sozialromantik [12]. Wesentliche Schwächen der bisher entwickelten Modelle sind dabei:

- Linearität – Cyber Security wird als eine Abfolge von Ereignissen und Maßnahmen angesehen, die einem Zielzustand zustrebt. Bei Erreichen des Zielzustands gelten die betreffenden Sicherheitskonzepte als umgesetzt, mithin sei ein „sicherer“ Zustand erreicht.
- Inkorrektes Bezugssystem – Cyber Security richtet sich, zumindest nach maßgeblichen Definitionen wie [13] entweder auf die Technik oder auf die organisationsinternen Regelungen. Technik wird dabei als definiertes, Regelung als normatives Element wahrgenommen. Die Interaktion mit dem Menschen ist ausdrücklich nicht Gegenstand der Cyber Security, da ein normgerechtes und technisch fehlerfreies Verhalten vorausgesetzt wird.
- Geschlossenheitsannahme – Cyber Security richtet sich auf organisationsinterne oder nationalstaatliche Strukturen. Dies verkennt die relative Endlichkeit der Regelungen und der Technik (Beschränkung auf den jeweiligen Machtbereich) ebenso wie die offenkundige Freizügigkeit (auch krimineller) Menschen. Beispiele für ein Durchbrechen der Geschlossenheitsannahme sind u. a. Grenzübertritt in ein anderes Land, Wechsel zu einem anderen Unternehmen, Nutzung von Drittparteien etc.

- Best-Practice-Annahme – Cyber Security geht von der Prämisse aus, daß die graduelle Reduzierung von Schwachstellen und das „Machbare“ das Risiko des Cyber Crime nachhaltig senken. Dies gilt nur bedingt, da Cyber Crime sich in wesentlichem Maße auf das jeweils schwächste Glied in der Kette konzentriert und die ausreichend geschützten Ziele umgeht.
- Integritätsannahme – Regelwerk und Schutzmechanismen gehen von der Annahme aus, daß im Geltungsbereich von Konzepten der Cyber Security integre und regeltreue Menschen (und zwar nur solche) vorhanden sind. Diese Fiktion dient zwar der Aufrechterhaltung der Ordnung, doch führt gerade das Postulat „in unserer Organisation vertraut man einander“ zu erhöhten Risiken.
- Allwissenheitsannahme – sowohl organisatorisch-unternehmerische als auch staatliche Konzepte der Cyber Security gehen von einer (mittelfristig) vollständigen Erkennung von Delikten im Cyber Crime aus. Das bestehende Dunkelfeld wird zwar im Grunde erkannt [14], geht jedoch oft nicht in Planung und Maßnahmenbildung ein.
- Beherrschbarkeitsannahme – Cyber Security geht bis dato von einer nahezu vollständigen Kontrolle und Beherrschung der Situation aus. Ansätze wie eine „Internetabschaltung“ [15] zeigen das Bestreben, durch politisch-legislative Initiativen die Illusion einer vollständigen Kontrolle aufrechtzuerhalten.

Ausschlaggebend für Erfolg oder Versagen in der Cyber Security ist die sehr unterschiedliche Perspektive der Staaten beziehungsweise Organisationen und der Menschen als Individuen. Auch organisatorische, nationale und supranationale Strukturen werden letztlich von Menschen gebildet, die neben einer organisationsbezogenen Sicherheit zweifellos eine eigene, sehr persönliche Wahrnehmung haben. Die resultierende Divergenz der Konzepte wird im folgenden nachgewiesen.

2.1 Sicherheitsmanagement aus Organisationssicht

Sowohl Organisationen als auch Nationalstaaten verfügen in der Informationssicherheit und folglich auch in der Cyber Security über ein sehr breites Instrumentarium an Gesetzen, Normen und Standards. Die Technik steht dem in nichts nach; eine Vielzahl von Herstellern bietet Hardware- und Softwarelösungen für fast jeden Anwendungsfall an. Konzepte im organisatorischen Bereich besitzen die folgenden generischen Komponenten:

- Compliance-Komponente: verbindliche Regelungen (extern oder intern legitimiert) werden in hierarchischer Form definiert, kommuniziert und überprüft. Verstöße zeitigen interne oder externe Sanktionen.

- Governance-Komponente: verbindliche Empfehlungen und Hinweise, die abstrakte Werte formulieren und in ähnlicher Weise wie Compliance-Regelungen behandelt werden.
- Risiko-Komponente: die Sicherheit wird zumindest in Teilen an das Risikomanagement angelagert, um weitgehend präventive Maßnahmen zu einer Verminderung der wahrgenommenen Risiken zu treffen.
- Technische Komponente: die sogenannte „GRC-Triade“ wird durch technische Einzellösungen ergänzt, die zur Unterstützung einzelner Prozesse oder Vorschriften dienen, beispielsweise in einem Identity- und Access-Management-System.

Die IT-Nutzung in Organisationen unterliegt häufig Restriktionen, denen sich der einzelne Mensch durch Kenntnisnahme und Unterzeichnung zu unterwerfen hat. Wirtschaftliche Abwägungen führen überdies dazu, daß Cyber Security mit begrenzten Budgets ausgestattet ist [16]. Ausgestaltung und Überwachung der Sicherheitsrichtlinien obliegen einem in der Regel kleinen Kreis von Menschen in entsprechenden Abteilungen.

Augenscheinlich [17] hat dieses Modell bereits jetzt seine Grenzen erreicht. Verbesserungen in der Cyber Security sind nur noch mit stark erhöhtem Aufwand realisierbar, und die nicht von der Hand zu weisende, aber regelmäßig verkannte Gefahr des Cyber Crime aus dem Inneren der Organisation [18] kann das „GRC“-Geschehen ebenso wie die Technik sehr rasch ad absurdum führen. Sowohl technische als auch organisatorische Lösungen sind mithin notwendige, aber nicht hinreichende Bedingung für den Schutz gegen Cyber Crime.

2.2 Persönliches „Sicherheitsmanagement“

Menschliches Verhalten zeigt im Hinblick auf Cyber Security eine extreme Streuung, die eine wissens- und generationenbedingte Typisierung ermöglichen [19]. Strukturell befinden sich die meisten Menschen in einem technisch-organisatorischen Kontext, der durch das Unternehmens- oder Organisationsgeschehen fremdbestimmt ist. Daraus resultiert zum einen die zwingende Unterwerfung unter eher nicht reflektierte Regeln: Vorschriften ersetzen häufig die kritische Reflexion des eigenen Verhaltens, da sie keine alternativen Handlungen zulassen. Zum anderen bringt die Fremdbestimmung eine Schutzerwartung des Menschen an Dritte hervor: der Transfer der Verantwortung an eine andere Abteilung verpflichtet diese, den Schutz derjenigen zu gewährleisten, welche die Regeln befolgen.

Im privaten Umfeld ist der Mensch hingegen allein verantwortlich für Cyber Security. Risikowahrnehmung, -abwägung und Sicherheitsmaßnahmen obliegen dem Individuum. Bei gegebener Komplexität stellt diese Tatsache hohe bis sehr hohe Anforderungen an Menschen, die sich aktiv im Cyberspace betätigen und dort geschäftliche Transaktionen durchführen.

Das persönliche Sicherheitsmanagement wird daher im privaten Bereich oft nur rudimentär umgesetzt. Nach der in [19] vorgeschlagenen (erweiterten) Typisierung reagieren „Digital Ignorants“ mit einem faktischen Rückzug aus bestimmten Angeboten und Plattformen im Cyberspace; sie sind dadurch weitgehend vor Cyber Crime geschützt. Die „Digital Immigrants“ zeigen trotz reger Teilnahme am Geschehen im Cyberspace einen nahezu perfekten Umgang mit der Cyber Security, zumal sie über die vollständige Erfahrung aus der Entstehungszeit des modernen Cyberspace verfügen. „Digital Natives“ und ihre Nachfolger sind im Gegensatz dazu hochgradig gefährdet, da sie nicht mehr über das notwendige tiefe Wissen in der IT verfügen.

Im Rückbezug auf den Menschen im Organisationskontext setzt sich diese Typisierung fort. Möglicherweise erklärt sich hieraus auch der Umstand, daß trotz umfassender GRC-Vorgaben immer wieder menschliche Fehler vorkommen, die im nachhinein als fahrlässig oder ignorant erscheinen. Im Forschungsgebiet der technischen Risiken zeigen schon frühe Arbeiten [20, 21, 22], daß sowohl unabsichtliches als auch vorsätzliches Fehlverhalten in sehr komplexen Umgebungen vorhersagbar ist; für die Cyber Security muß also zwingend auch normabweichendes Verhalten in die strategischen Überlegungen einbezogen werden.

3 Angriffsvektoren und Ziele

Zieldefinition und Zielerfassung haben in den letzten Jahren einen tiefgreifenden Wandel erfahren. Von der ursprünglichen Absicht des „ethical hacking“ über Diebstahl und Erpressungsdelikte bis hin zu DoS, DDos und Botnets definieren Cyber Criminals immer komplexere Ziele. Ein Botnet-Betreiber beispielsweise begeht selbst keine Delikte, sondern vermietet lediglich die tatfördernde Infrastruktur. In der Grauzone zwischen Cyber Crime und Cyber Warfare dienen kriminelle Organisationen – gegen entsprechendes Entgelt – durchaus auch politischen Zielen, die durch ein nationalstaatliches Mandat gesetzt werden: „Onward Cyber Mercenaries“. Temporäre, opportunistische Täterstrukturen sind die Folge der Konvergenz von Cyber Crime und Cyber War. Die Motivation des jeweiligen Angriffs ist demnach ebenso schwer zu bestimmen wie die „richtige“ Gegenreaktion, die organisatorisch, zivilstaatlich oder militärisch erfolgen kann [23].

Die Zielerfassung ist ebenfalls vielfältiger geworden. Kleinere Unternehmen und Einzelpersonen sind nun häufiger Ziel eines Angriffs, und die Schadenshöhe im Einzelfall steigt [24]. In Großunternehmen, die durch zentrale Sicherheitskonzepte abgedeckt sind, verbleiben gleichwohl Einzelziele, die sich durch unzureichende Einhaltung der Vorschriften oder durch menschliche Schwächen ergeben und teilweise jahrelang bestehen. Art und Umfang des Ziels sind dabei vorwiegend im Bereich des Zahlungsverkehrs (85%) angesiedelt [25].

Die resultierenden Angriffsvektoren sind im Ergebnis breiter angelegt als in den vergangenen Jahren. Die Mittel der Wahl sind zu 48% Mißbrauch, 40% Hacking und 38% Malware [26], bei gleichzeitigem Rückgang der „social attacks“. Gleichzeitig ist laut [26] der Malware-Vektor für über 94% der Datenverluste verantwortlich, also bei weitem die effektivste Angriffsmethode. Der Schwierigkeitsgrad des jeweiligen Angriffs (unabhängig vom gewählten Mittel) liegt nur in 15% der Fälle auf hohem Niveau, jedoch zu 41% auf geringem oder sehr geringem Niveau. Sowohl die Vektoren als auch ihre vergleichweise triviale Nutzbarkeit deuten auf eine Verbreiterung des Angriffsgeschehens und eine überproportional steigende Anzahl von Tätern und Tätergruppen hin. [25] belegt überdies die stark steigende Anzahl der angreifbaren Plattformen, unter anderem durch die verstärkte Nutzung intelligenter mobiler Endgeräte.

Cyber Crime kann sich folglich neben traditionellen und neuen Angriffsvektoren auch zunutze machen, daß eine erleichterte Tatdurchführung nebst Multiplikation der möglichen Zielplattformen gegeben ist. Zusammenfassend liegt auf der Hand, daß nach den vorliegenden Daten ein nichtlineares Wachstum des Cyber Crime zu erwarten ist.

4 Asymmetrie und Angreifbarkeit

Aus der Lage der Informationssicherheit und den veränderten Angriffsvektoren resultiert eine tiefgreifende Asymmetrie. Die Absicherung einer Organisationsumgebung erfordert einen wesentlich höheren Aufwand als der Angriff einer Einzelperson oder Kleingruppe; erhöhte Regel- und Kontrolldichte wird durch unorthodoxes Vorgehen von Tätergruppen neutralisiert und nachgerade ad absurdum geführt. In Verbindung mit der durch nationale Grenzen und politische Hemmnisse geprägten Sicherheitslage entsteht eine wesentlich höhere Angreifbarkeit für kritische Infrastrukturen, aber auch für Einzelpersonen. Aus der Perspektive des Cyber Crime sind letztere bevorzugte Ziele, da sie sowohl technisch als auch sozial leichtere Angriffsziele bieten.

Bereits jetzt zeigt sich in der Praxis, daß das Angriffsgeschehen eine Verlagerung in genau diese Richtung erfährt. Diffus strukturierte Netzwerke wie „Anonymous“ oder „LulzSec“ nutzen verteilte Kleingruppen, um auch große und generell gut geschützte Ziele anzugreifen. Zeitgleich sind breit angelegte Angriffswellen auf Einzelpersonen zu beobachten, die durch entsprechende Malware vorbereitet werden. Häufigkeit und Intensität beider Angriffsformen steigen sprunghaft an. Das herrschende Paradigma einer Sicherheitsstrategie rein auf Organisationsebene wird schrittweise zersetzt, da auch sehr aufwendige Konzepte und Lösungen offenkundig nicht mehr ausreichen, um die zunehmende Angreifbarkeit auf der individuellen Ebene zu neutralisieren. Das Schutzziel „Organisationseinheit“ muß sogar insgesamt hinterfragt werden, zumal die Außengrenze einer Organisation nicht mehr mit Sicherheit bestimmt werden kann.

In Szenarien mit Beteiligung verschiedener Cloud-Provider oder einer Verbindung hin zur individuellen Nutzung sozialer Netzwerke auf Unternehmensrechnern darf nicht länger davon ausgegangen werden, daß die Sicherheit in ausreichendem Maße gegeben ist.

Asymmetrie und Angreifbarkeit gehen mit einer erheblichen Ausweitung des Begriffs „Unternehmen“ einher. Betriebswirtschaftliche Überlegungen führen immer häufiger zu einer kaskadierenden Auslagerung auch kritischer Geschäftsprozesse und Datenbestände [27]. Die Nutzung öffentlicher Clouds spielt dabei im Hinblick auf Cyber Crime eine bedeutsame Rolle, da sie zum einen ein erhöhtes Agglomerationsrisiko mit sich bringt, zum anderen die Feststellung einschlägiger Taten erschwert oder unmöglich macht. Wenngleich namhafte Cloud-Provider durchaus große Anstrengungen hin zu einer Sicherung und Härtung der jeweiligen Umgebungen unternommen haben, ist dennoch eine erhöhte Attraktivität solcher Umgebungen für Angriffe nicht von der Hand zu weisen. Erschwerend aus Sicht der deutschsprachigen Länder sind die Geschäftsbedingungen im Cloud Computing mit weitreichenden Haftungsausschlüssen versehen [28], die hohe Hürden für eine rechtliche Verfolgung von Straftaten setzen. Delikte können so in einer Art „Grauzone“ begangen werden, in welcher der Geschädigte keine Möglichkeit, der Cloud Provider jedoch kein Interesse an einer nachhaltigen Verfolgung des Cyber Crime hat.

Zusammenfassend ist aufgrund der vielfältigen Veränderungen in der Praxis eine Abkehr vom bisher verfolgten Sicherheitsparadigma unumgänglich. Die Person als kleinste – und angreifbarste – Einheit im Sicherheitsgeschehen muß in den Mittelpunkt gerückt werden, um die vielfältigen Bedrohungen und Lücken bereits auf individueller Ebene schließen zu können. In den vorangegangenen Abschnitten wurde gezeigt, daß eine auf immer mehr Restriktionen und Kontrollen beruhende Sichtweise sich schon mittelfristig selbst ad absurdum führt, da die Kosten prohibitiv hoch sind. Mithin kann nur durch einen „bottom up“ Ansatz langfristig das gewünschte Sicherheitsniveau erreicht werden.

5 Lösungsansätze im Sicherheitsmanagement

Das vom Verband ISACA (Information Systems Audit and Control Association) erstmals 2010 veröffentlichte Sicherheitsmodell BMIS [29] verfolgt einen systemischen Ansatz in der Informationssicherheit. Ausgehend von [30] definiert das Modell statische Elemente und dynamische Verbindungen, die eine dreidimensionale Sicht auf das Sicherheitsgeschehen im Unternehmen ermöglichen. Abbildung 1 zeigt das Modell im Ausgangszustand.

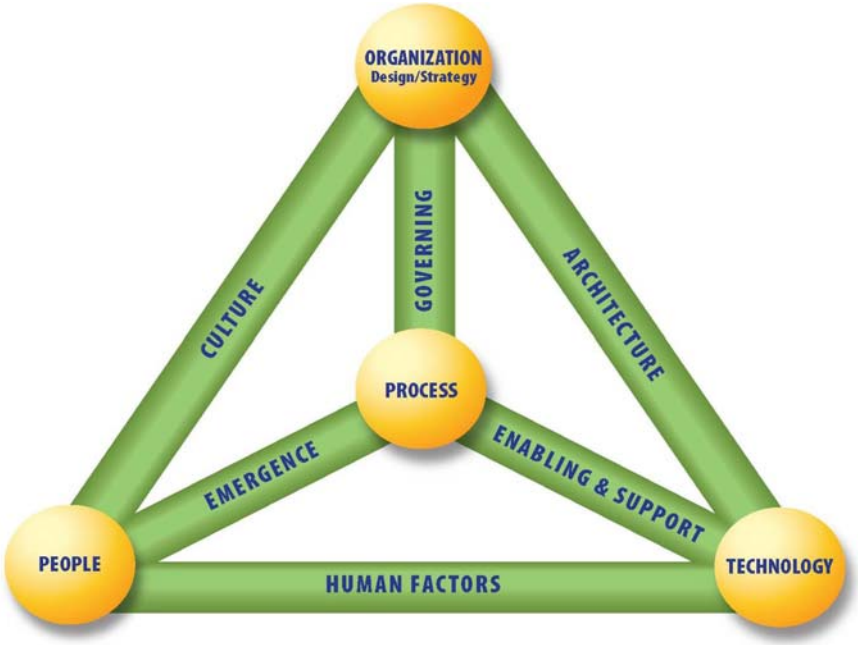


Abbildung 1: Business Model for Information Security (Quelle: ISACA)

Die auf Einzelpersonen bezogene Perspektive nach BMIS ergibt sich aus Abbildung 2. Das Element „People“ steht im Mittelpunkt, und die analytische Behandlung erfolgt über die zugehörigen Verbindungen zu den benachbarten Elementen.

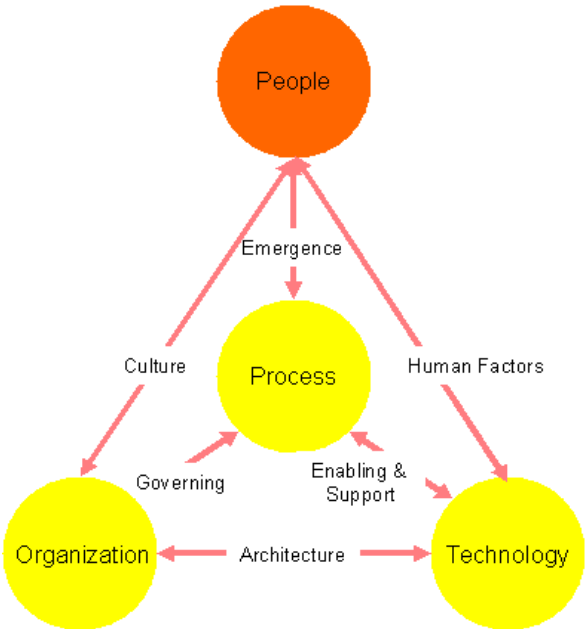


Abbildung 2: BMIS - personenzentrische Sicht

Die folgenden Abschnitte zeigen, wie ein individuelles Sicherheitsparadigma aus den Elementen und Verbindungen des BMIS hergeleitet werden kann. Dies dient einerseits der intensiven Auseinandersetzung mit dem individuellen Verhalten. Zum anderen lassen sich dadurch Strategien verfolgen, die explizit solche Probleme lösen, die sich aus der Verschiebung der Verantwortung in Richtung einer arbeitsteiligen Organisation ergeben.

5.1 Das Element „People“

Nach [29] entscheidet die Person im Kontext der Gruppe und der Organisation, ob und in welcher Form Beschränkungen, Kontrollen und Sicherheitsprozesse individuell akzeptabel sind. In der engen BMIS-Definition ist der Mensch von unterschiedlichen Strukturen im Unternehmen umgeben; an dieser Stelle ist die Definition zu erweitern. Im Sinne eines individuellen Sicherheitsansatzes ist dabei der Mensch auch im privaten Bereich von organisationsähnlichen Strukturen umgeben, die sich aus der Geschäftsbeziehung oder Vertragsbeziehung zu Dritten herleiten. Dies können soziale Netzwerke, Unternehmen oder andere Lieferanten und Dienstleister sein – allerdings obliegt es dem einzelnen, hieraus das jeweils richtige Vorgehen in der Sicherheit abzuleiten.

Anstelle der Organisation tritt in der persönlichen Sicherheit oft ein anderes Bezugssystem, das sich aus der gewählten peer group (Freunde, Familie, Verein etc.) erklärt. Der Mensch trifft anhand der Beurteilung des Umfelds Entscheidungen über das bestehende Risiko und resultierendes Verhalten. Bei meist unvollständiger Information über die tatsächliche Sicherheitslage sind diese Entscheidungen oft intuitiv, häufig auch durch minimalen Aufwand oder Umgehung bestehender Sicherheitsmaßnahmen. „Human error“, also menschliches Versagen, ist in diesem Umfeld nicht auszuschließen.

Diese Faktoren müssen in die Überlegung zu einer individuellen Sicherheitsstrategie einbezogen werden. Die dem Element „People“ benachbarten Elemente „Organization“ und „Process“ können nur dann ihre vollständige Wirkung im Sinne der Sicherheit entfalten, wenn die individuellen Schwächen minimal sind.

5.2 Kultur und die Verbindung zwischen Mensch und Organisation

Mensch und Organisation (oder privates Bezugssystem) sind über „Culture“ verbunden. Diese dynamische Verbindung kennzeichnet Werte, Erkenntnisse und Wissen, die über einen längeren Zeitraum eingeführt, verfestigt und tradiert werden.

Im Gegensatz zu einer Definition des Sollzustands durch die Verknüpfung „Governing“ betrachtet die kulturelle Sicht die tatsächliche Situation der Informationssicherheit, der menschlichen Wertesysteme und der faktisch gelebten Unternehmenskultur – die im übrigen nicht immer mit den durch Governance vorgegebenen Vorstellungen übereinstimmen muß.

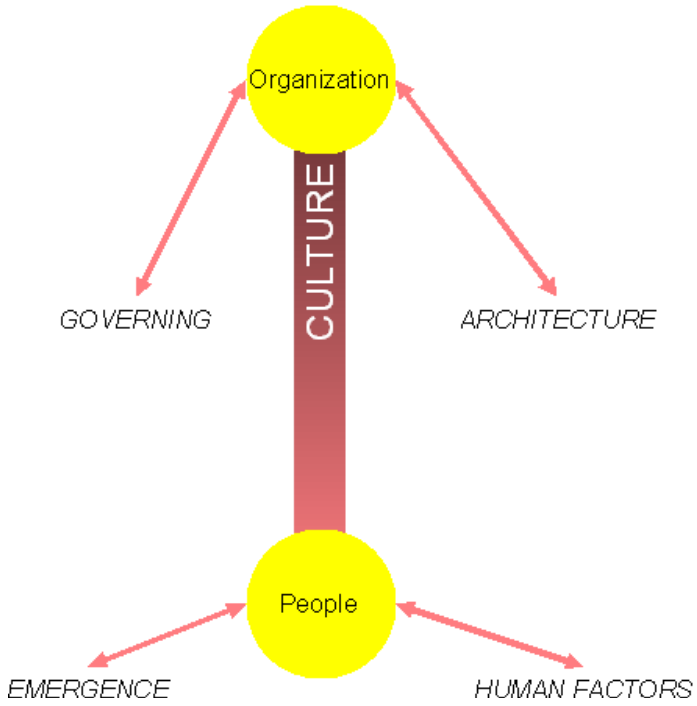


Abbildung 3: Kultur als Verbindung zwischen Mensch und Organisation

Die „Culture“-Verbindung führt häufig dazu, daß Einzelpersonen implizite Vorstellungen und Erwartungen pflegen, die nicht unbedingt mit der tatsächlichen Sicherheitslage übereinstimmen. Für ein individuell wirksames Sicherheitsmodell ist damit eine Leitkultur erforderlich, die unter anderem folgende Punkte überzeugend darlegt:

- Eigenverantwortung: auch innerhalb einer Organisation erschöpft sich die „Wunschkultur“ nicht in einer reinen Befolgung gegebener Vorschriften. Kritische Überprüfung im Sinne einer „high reliability organization“ [21] und selbstreflektierendes Vorgehen sind unumgänglich.
- Lern- und Hilfskontext: organisatorisches Umfeld und kulturelle Prägung ermöglichen sowohl umfassende Hilfestellung als auch Lernprozesse auf individueller Ebene. Im Gegensatz zur reinen Verregelung sicherheitsrelevanter Sachverhalte entsteht so die Verpflichtung zu einer aktiven Wissensaneignung und zur Eigensicherung.

- Kulturelle Grundwerte: aus Sicht der Organisation dienen Vorgaben der oberen Führung als Leitlinien für Mitglieder; im sozialen Umfeld können dies auch andere Personen mit entsprechender Vorbildfunktion sein. Die häufig gepflegte Ideologie des „do more with less“ und die Betrachtung der Sicherheit als Kostenfaktor sind ungeeignete kulturelle Grundwerte, wenn Täter sich dem „do more with more to get more“ verschrieben haben.

Die umgebende Kultur kann somit für den einzelnen Menschen nur Angebot und Bestätigung sein, statt wie bisher einen normativen Anspruch aus Sicht der Organisation zu stellen. Eine individuelle Sicherheitsperspektive kann nur dann entwickelt werden, wenn keine zunehmende Entmündigung durch eine anschwellende Kontroll- und Normenlast stattfindet. Es ist entscheidend wichtig, hier eher eine Vereinfachung in Richtung weniger, aber durchgreifender kultureller Werte zu versuchen.

5.2 Sicherheitsrelevante Prozesse und Emergenz

Die „Emergenz“-Verknüpfung erweitert das BMIS um das Element des Zufalls und der Nichtvorhersagbarkeit, ferner durch die Integration echter Emergenz. Die Forschungslage deutet darauf hin, daß systemische Emergenz häufig ein spontanes Phänomen ist, das in Teilen des Systems oder im Gesamtsystem Veränderungen hervorruft. In der Ausführung sicherheitsrelevanter Tätigkeiten und Prozesse haben einzelne Menschen fast immer einen Ermessensspielraum, der im Gegensatz zu vollständig automatisierten Systemen auch durch maximale Kontrolldichte nicht beherrschbar ist. In Gruppen und größeren Einheiten konvergiert bisweilen das menschliche Verhalten: nach einer Phase der Anpassung werden gegebenenfalls Prozesse anders interpretiert, augeführt und teilweise neu geschaffen. Gleichzeitig entsteht als Gegenpol eine Divergenz zum Sollzustand eines oder mehrerer Prozesse, beispielsweise gegenüber Erwartungen hinsichtlich Governance oder Compliance. Sicherheitsstrategien im Kollektiv tendieren zu einer Erhöhung der Kontrolldichte und zu Sanktionen, um das Phänomen der Emergenz zu begrenzen. Für einzelne Menschen ergibt sich aus dieser Tendenz häufig der Eindruck bürokratischer Arbeitsbehinderung, nebst Reaktionen von Frustration bis Widerstand.

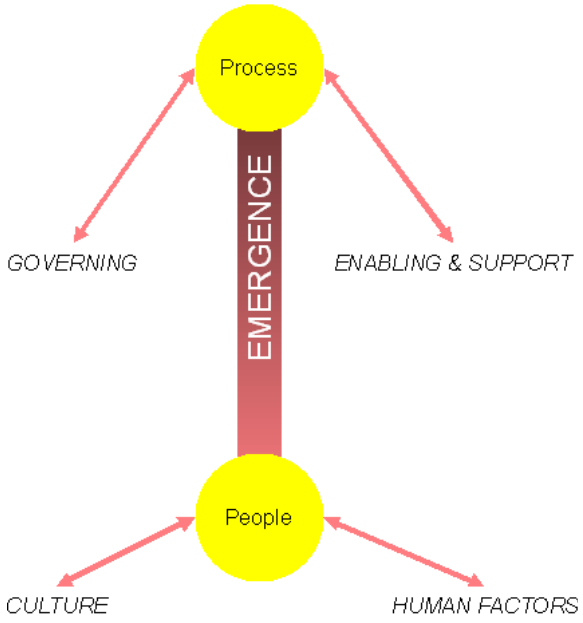


Abbildung 4: Emergenz in der Interaktion zwischen Mensch und Prozeß

In der Informationssicherheit adressiert das BMIS typische Problemstellungen wie die kulturelle Verschiebung von „digital ignorants“ zu „digital natives“ und deren Auswirkungen auf die Gestaltung von Geschäftsprozessen, aber auch den Übergang von hierarchischen Sicherheitsmodellen (Zentralautorität) zu vernetzten Sicherheitsstrukturen. Emergenz ist überdies dort evident, wo gegenüber zentralen Vorgaben und starren Sicherheitsstrukturen eine Individualisierung und Privatisierung des Sicherheitsempfindens stattfindet, die Individuen und Gruppen zu mehr Verantwortung, aber auch zu mehr Distanz von zentralen Leitlinien veranlaßt. Für eine personenbezogene, nachhaltige Informationssicherheit ist es erforderlich, Emergenz als Möglichkeit zur intelligenten Verbesserung zu begreifen:

- Verkürzung / Vereinfachung von Prozessen: die Komplexität des jeweiligen Prozesses ist zu überprüfen. Wenn die Vereinfachung zu unkalkulierbaren Sicherheitsrisiken führt, ist dies erfahrungsgemäß auch vermittelbar und führt zu einer Rückkehr zum bisherigen Prozessverlauf.
- Umgehung / Workarounds: die Gründe für die fehlende Akzeptanz des Prozesses sind zu analysieren. Im Regelfall ist jede Umgehung ein Anzeichen für ineffiziente Prozessgestaltung, jedoch abzugrenzen von menschlichen Phänomenen wie Leichtsinn oder Bequemlichkeit.

- Fehlerhafte / defizitäre Ausführung: Design des Prozesses, Bezug des Prozesses zur Unternehmenskultur und zu vor- und nachgelagerten Prozessen ist zu überprüfen. Neben reinen Mißverständnissen oder Kommunikationsfehlern kann die Sollvorstellung unter Umständen in der Praxis nicht erfüllt werden.

Während im Unternehmensumfeld ein definierter Sollzustand in bezug auf sicherheitsrelevante Prozesse besteht, ist dies im privaten Umfeld der Menschen weniger gegeben. Emergenz manifestiert sich hier in anderer Form, beispielsweise durch konvergentes Verhalten im sozialen Bezugssystem oder in bestimmten Altersgruppen. In allen Fällen zeigt sich jedoch, daß Emergenz zunächst durch Individuen, dann durch Gruppen und deren Verhalten sichtbar wird. Diese Tatsache ist deswegen hoch zu bewerten, weil gerade in der Informationssicherheit durch die emergenten Phänomene erheblich Verbesserungen erzielt wurden und werden. Zudem wird unter Beweis gestellt, daß im Konzept einer individualisierten Sicherheit der Prozeß dem Menschen dient – nicht umgekehrt.

5.3 Nutzung von Technologien und Auswirkungen für Personen

Die Verknüpfung „Faktor Mensch“ verbindet die Präsenz unterschiedlicher Technologien mit ihrer Nutzung durch Menschen im weitesten Sinne. In vielen Anwendungsfällen wird Information durch Menschen in unerwarteter Weise genutzt, teilweise auch gegenläufig zu den ursprünglichen Zielen des Informationsanbieters. In einigen Fällen entsteht hierbei eine unerwartete Innovation, die sich auf Dauer verfestigen kann. Aus Sicht der Informationssicherheit führt die Nutzung der Technologie zu zahlreichen Herausforderungen und Bedrohungen – dies gilt insbesondere in jenen Fällen, in denen unabsichtliches oder vorsätzliches Verhalten die Sicherheitsmaßnahmen umgeht oder vollständig außer Kraft setzt. Die Schnittstelle zwischen Mensch und Technologie, insbesondere im Bereich der „Usability“, sekundär auch im Bereich der „Intuitiveness“, ist zentrales Element für eine praktische Gewährleistung der Informationssicherheit unter Berücksichtigung des menschlichen Verhaltens. Existierende Sicherheitsmodelle haben hier entscheidende Schwächen, da sie a priori von einer Einhaltung einmal eingeführter Vorgaben und Vorschriften ausgehen. Die resultierenden Praxisprobleme konzentrieren sich folgerichtig auf Fälle der Nichteinhaltung oder Umgehung von Sicherheitsmaßnahmen, die bei Anwendung älterer Sicherheitsmodelle auftreten. Implizite Annahme ist, daß das jeweils gültige Modell Priorität hat und im Regelfall eine Anpassung des menschlichen Verhaltens erzwingen will.

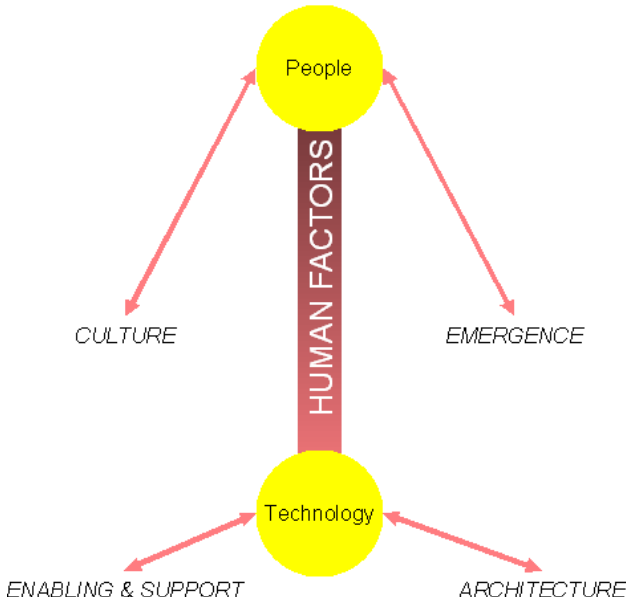


Abbildung 5: BMIS - Menschliche Faktoren

Aufwand und Investitionen richten sich nach dieser Logik auf eine Durchsetzung des abstrakten Modells gegen die bestehenden Verhaltensformen oder tradierte betriebliche Abläufe. Passiver oder aktiver Widerstand gegen die überhand nehmende Anzahl von Vorschriften und Sicherheitsrichtlinien ist jedoch in der Praxis immer häufiger und immer deutlicher zu beobachten. An dieser Stelle führt das BMIS eine Umkehrung der Sichtweise herbei, indem zuerst das menschliche Verhalten als gegebene Tatsache vorausgesetzt wird; nur unter Berücksichtigung dieser Prämisse können Modelle und technische Bedingungen eingeführt werden, die eine ausreichende innerbetriebliche Akzeptanz haben.

- Usability: Bedienbarkeit und einfache Ablaufmuster in der Sicherheit sind zentrale, aber oft vernachlässigte Elemente. Beispiele wie komplexe Passwörter zeigen, wie aus einer unkomfortablen Bedienung sehr rasch Ablehnung und normabweichendes Verhalten entstehen kann.
- Intuitiveness: Ziel ist ein geringerer Aufwand für die Einarbeitung in sicherheitsrelevante Sachverhalte, ferner die weitgehende Standardisierung in Richtung einer allgemein verständlichen und anerkannten Handhabung. Proprietäre Sicherheitslösungen führen häufig zu einem fehlenden Verständnis und zu mangelnder Akzeptanz der Lösung an sich.
- Positive Rückkopplung: der Sicherheitsgewinn durch ein erwünschtes Verhalten beziehungsweise eine erwünschte Nutzung technischer Lösungen muß unmittelbar erkennbar sein. Die Frage „Warum muß ich das tun?“ bedarf in der Praxis einer überzeugenden Antwort.

6 Schlußfolgerungen und Ausblick

Aus den Schwächen bestehender Sicherheitsmodelle ergibt sich eine Verschiebung von der Vorstellung einer Sicherheit im Kollektiv hin zur Sicherheit des Individuums. Die Zielrichtung des Cyber Crime verstärkt die Notwendigkeit einer personenbezogenen Sichtweise, da der einzelne Mensch auch im Kontext einer Organisation und ihrer Vorschriftenlage stets angreifbar bleibt. Auch bei hoher bis sehr hoher Kontrolldichte sind in der Praxis abweichende Verhaltensweisen und menschliche Fehler unvermeidlich; daraus folgen Schwächen, die durch neue Angriffsvektoren und asymmetrische Täterstrukturen genutzt werden können.

Daraus folgt, daß ein systemischer Ansatz in der Cyber Security benötigt wird. Anhand des BMIS kann gezeigt werden, wie durch den Ausgangspunkt „People“ nebst Betrachtung der davon ausgehenden dynamischen Verbindungen eine individuelle Sicherheit geschaffen wird. Der Ansatz einer fehlertoleranten und auf den Menschen gerichteten Denkweise weicht dabei vom zentralistischen Paradigma ab und akzeptiert a priori jene Schwächen, die in traditionellen Sicherheitsmodellen zu den bekannten Problemen führen.

Gestützt werden diese Schlußfolgerungen durch die augenscheinliche Häufung kritischer Sicherheitsvorfälle, die in der jüngsten Vergangenheit auch als gut geschützt geltende Umgebungen betreffen und regelmäßig zu einem Taterfolg führen. Nur durch die Stärkung der individuellen Sicherheit kann eine Gegenposition geschaffen werden, die sich positive menschliche Eigenschaften wie rasches Lernen und flexiblen Umgang mit unerwarteten Situationen zunutze macht. Hier erweist sich die dynamische und systemische Sicht des BMIS als entscheidender Vorteil.

Zukünftige Ansätze in der Cyber Security werden sich zwangsläufig am Menschen als kleinster und zugleich wichtigster Einheit im Sicherheitsgeschehen orientieren müssen. Während die traditionelle Cyber Security immer häufiger in unhaltbaren Einschränkungen oder prohibitiven Kosten endet, erschließt sich durch die Umkehrung des zugrunde liegenden Paradigmas eine Antwort auf die verschärfte Bedrohungslage.

[1]vgl. u. a. Dt. Bundestag (2010): „Dem Staat kommt die Aufgabe zu, das Internet als freiheitliches Medium zu schützen. Die Bürger bauen darauf, dass der Rechtsstaat durch Rahmenbedingungen die Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellt. In autoritär geführten Staaten, in denen die klassischen Medien zensiert und staatlich kontrolliert werden, können wir beobachten, welche Chancen das Internet für Demokratie, Meinungsfreiheit und eine unabhängige Berichterstattung birgt." - man beachte den (wohl unfreiwilligen) Doppelsinn durch Orientierung an autoritär geführten Staaten. Daselbst weiters: „Kinder und Jugendliche, die mit den neuen Technologien des digitalen Zeitalters aufwachsen, nutzen diese anders als die Generation ihrer Eltern. Dennoch müssen sie auf möglichen Gefahren der digitalen Gesellschaft vorbereitet, ihre Fragen beantwortet und zu einem sicherheitsbewussten Verhalten hingeführt werden. Im Jugendschutz sind noch Verbesserungen möglich. Dabei ist uns bewusst, dass die Gefahren für Kinder und Jugendliche durch Verbote oder technische Maßnahmen nicht ausgeschlossen werden können. Deshalb muss die Medienkompetenz auch von Kindern, Jugendlichen und Eltern gestärkt werden." In Fragen der Gefährdung und Kompetenz wären wohl die Eltern an erste Stelle zu setzen, aus deren Generation auch die unterzeichnenden Politiker (darunter niemand mit IT-Fachwissen) stammen. (Hervorhebungen durch den Autor).
[2]zur Begriffsklärung vgl. u. a. Wikipedia [de.wikipedia.org/hacker]
[3]hierzu kontrovers Weiss (2011) und dortige Verweise; implizit auch bei (o. V.) epd (2011) als Zitat der dt. Bundesfamilienministerin. Obgleich die sogenannte „Internet-Gemeinde" zweifellos die Mehrheit der Bevölkerung in Deutschland bildet, reflektieren politische Kommentare noch immer eine deutlich eingefärbte Skepsis.
[4]siehe insbesondere die Kontroverse um Internet-Sperren im Jahr 2009 und zugehörige Quellen.
[5]Engl. „nanny state", vgl. Macleod (1965) zitiert in Ayto (2006).
[6]Die 2011 erschienene Studie „Risk/Reward Barometer" [www.isaca.org] thematisiert erstmals den zunehmenden Druck auf Unternehmen, auch persönliche Geräte der User (in erster Linie iPhones und dergleichen) zuzulassen. Unter dem Stichwort „BYOD" (Bring Your Own Device) scheint sich hier eine umfassende Änderung abzuzeichnen.
[7] Noch im Jahr 2011 führte eine große internationale Wirtschaftsprüfungsgesellschaft mit physisch neuen Laptops Windows Vista ein. Das bereits seit 2010 verfügbare Windows 7 soll Ende 2012 schrittweise eingeführt werden.
[8] Ayling, J. "Criminal organizations and resilience." International Journal of Law, Crime and Justice 37, no. 4 (2009): 182–196. - „While dealing in illegal products and having to dodge state bullets increases a criminal organization's vulnerability compared with a legitimate business, sometimes not having to 'play by the rules' may decrease vulnerability."
[9]unter anderem COBIT, RiskIT und ValIT, ferner ISO 27001 und nachgelagerte Normen; vgl. [www.isaca.org]
[10] Washington, D. W. Onward Cyber Soldiers. Time Magazine, 21. August 1995
[http://www.time.com/time/magazine/article/0,9171,983318,00.html]
[11] vgl. die anläßlich der Verurteilung des Hackers Kevin Mitnick ausgesprochene gerichtliche Verfügung, er dürfe sich keinem Computer auf weniger als 15 Fuß (etwa 5 Meter) nähern; siehe United States of America vs. Kevin Mitnick, 145 F.3d 1342, No. 97-50365. D.C. No. CR-95-00603-MRP-1., 20. Mai 1998, hier insbes. Ziffer 3. Interessant erscheint hier vor allem die Wirkungslosigkeit der Maßnahmen, da Mitnick auch nach seiner Veurteilung sehr viele Möglichkeiten eines indirekten Zugangs hatte; der mit der jeweiligen Genehmigung betraute „Probation Officer" dürfte nicht in der Lage gewesen sein, die jeweiligen Ansuchen auch nur ansatzweise in ihrer vollen Tragweite zu erfassen. [http://openjurist.org/145/f3d/1342/united-states-of-america-v-mitnick]
[12] vgl. u. a. Kleinwächter (2009), Otto (2009) in Bisky et. al. (2009) zur eher „linken" Position in Deutschland.
[13] vgl. Niggemeier, Präsentation des Bundesamts für Sicherheit in der Informationstechnik anläßlich des BITKOM-Arbeitskreises Sicherheitstechnologien, Frankfurt, 26. Mai 2011.
[14] vgl. BSI (2005) S. 18f stellvertretend für die reichhaltige Literatur zu Dunkelfeldstudien: „Vorfälle mit IT-Bezug sind häufig geeignet, generell das Vertrauen in die betroffenen Unternehmen zu schmälern. Entsprechend gering ist die Bereitschaft, solche Vorfälle überhaupt zu melden. [...] Vorfälle mit IT-Bezug werden häufig erst dann zu schweren Schäden führen, wenn IT-Einrichtungen nicht verantwortungsbewusst administriert wurden. Nicht selten dürfte bei den Verantwortlichen deshalb die Bereitschaft, an der Aufklärung mitzuwirken, gering sein."
[15] Der vielzitierte „Kill Switch" zur Abschaltung des nationalen (und möglichst internationalen) Internets wurde sowohl von US-Präsident Obama als auch von der dt. Bundeskanzlerin Merkel gefordert. Es ist unklar, was beide mit einer solchen Abschaltung bezwecken, denn Cyber Crime kann sowohl offline als auch mit entsprechender Latenz durchgeführt werden. Bei einer tatsächlichen Abschaltung dürfte sich viel eher die Frage stellen, wie lange diese unter wachsendem Druck der Bevölkerung und der Wirtschaft überhaupt aufrechterhalten werden kann.
[16] vgl. PwC, The Global State of Information Security, 2011: „As global economic conditions continue to fluctuate, information security hovers in the balance—caught between a new hard-won respect among executives and a painstakingly cautious funding environment."

[17] vgl. u. a. PwC (2011), Ernst & Young (2010) und andere einschlägige Studien.
[18] Moore et. al. (2008) für kritische Infrastrukturen, Osterheider (2007) zur Typisierung des Innentäters, Mokros (2007) zur Prävention. Bedenklich erscheint insbesondere die weitgehende Konvergenz der Persönlichkeitsmerkmale: der Grat zwischen erfolgreichem Manager und erfolgreichem Psychopathen ist schmal.
[19] Die Typisierung in „immigrants“ und „natives“ wurde durch Prensky (2001a, 2001b) erstmals vorgeschlagen; Erweiterungen durch den Autor.
[20] Lagadec, P. Major Technological Risk. Oxford: Pergamon Press, 1982.
[21] Perrow, C. Normal Accidents: Living with High-Risk Technologies. New York: Basic Books, 1984.
[22] Reason, J. Human Error. Cambridge: Cambridge University Press, 1990.
[23] Die resultierende Unsicherheit zeigt sich zum Beispiel in den USA: „Culpability, military planners argue in internal Pentagon debates, depends on the degree to which the attack, or the weapons themselves, can be linked to a foreign government. That's a tricky prospect at the best of times.“, Wall Street Journal vom 31. Mai 2011.
[24] vgl. PwC (2011) stellvertretend für die einschlägigen Studien.
[25] vgl. Trustwave (2011), S. 4.
[26] vgl. U. S. Secret Service (2010), S. 20.
[27] vgl. ISACA Risk/Reward Barometer 2011.
[28] vgl. stellv. die Geschäftsbedingungen der Firma Amazon - „You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content.“, ferner Abschnitt 11 „Limitations of Liability“.
[29] Business Model for Information Security (BMIS), vgl. ISACA (2010, 2011)
[30] vgl. Kiely und Benzel (2006).

Literatur

Ayling, J. “Criminal organizations and resilience.” International Journal of Law, Crime and Justice 37, no. 4 (2009): 182–196.

Ayto, J. Movers and shakers: a chronology of words that shaped our age. Oxford, UK: Oxford University Press, 2006.

Bisky, L., K. Kriese, J. Scheele (Hrsg.). Medien - Macht - Demokratie: Neue Perspektiven. Rosa Luxemburg Stiftung, Texte, Nr. 54. Berlin: Karl Dietz Verlag, 2009.

Deutscher Bundestag. Einsetzung einer Enquete-Kommission „Internet und digitale Gesellschaft“; Antrag der Fraktionen CDU/CSU, SPD, FDP und Bündnis 90 / Die Grünen. Anlage V 039/10, 24.02.2010.

Bundesamt für Sicherheit in der Informationstechnik. Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen. Bonn: BSI, August 2005.

Ernst & Young. Borderless Security – Global Information Security Survey 2010.

ISACA. Business Model for Information Security. Rolling Meadows, IL: ISACA, 2010.

ISACA. Creating a Culture of Security. Rolling Meadows, IL: ISACA, 2011.

ISACA. Risk / Reward Barometer 2011. Rolling Meadows, IL: ISACA, 2011.

Kiely, L., T. Benzel. Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs. University of Southern California / Marshall School of Business, 2006.

Lagadec, P. Major Technological Risk. Oxford: Pergamon Press, 1982.

Mokros, A. “Die integere und loyale Persönlichkeit: Wie man vermeidet, potenziell betriebsschädigende Personen einzustellen”. Präsentation beim Workshop des Instituts für Psychologie und Sicherheit, Aschaffenburg, 24. Juli 2007.

Moore, A. P, D. M. Cappelli, R. F. Trzeciak. The “Big Picture” of Insider IT Sabotage Across U. S. Critical Infrastructures. Technical Report. Carnegie Mellon University, May 2008.

Osterheider, M. “Meisterhafte Manipulatoren und Betrüger: Psychopathische Persönlichkeiten im Unternehmen erkennen”. Präsentation beim Workshop des Instituts für Psychologie und Sicherheit, Aschaffenburg, 24. Juli 2007.

o. V. “Pentagon: Online Cyber Attacks Can Count as Acts of War - WSJ.com.” Newspaper. Wall Street Journal, 31. Mai 2011.

o. V. Schröder – Internet-Gemeinde in Jugendschutz-Debatte einbinden, in epd Nr. 33a, 16.02.2011. [http://www.fsf.de/fsf2/aktivitaeten/bild/medien_impuls/20110215_jugendschutz/epd_medien_2011_02_16.pdf].

Perrow, C. Normal Accidents: Living with High-Risk Technologies. New York: Basic Books, 1984.

Prensky, M. “Digital natives, digital immigrants Part 1.” On the Horizon 9. Jg., Nr. 5. NCB University Press (2001): 1–6.

PriceWaterhouseCoopers. The Global State of Information Security Survey. PwC, 2011.

Reason, J. Human Error. Cambridge: Cambridge University Press, 1990.

Trustwave. Global Security Report 2011.

U. S. Secret Service, Verizon. 2010 Data Breach Investigations Report. U. S. Secret Service, 2010.

Washington, D. W. Onward Cyber Soldiers. Time Magazine, 21. August 1995
[http://www.time.com/time/magazine/article/0,9171,983318,00.html]

Weiss, M. „Günter Krings (CDU): ‘Internetgemeinde. Das klingt schon nach Sekte.’“, neunetz.com
[http://www.neunetz.com/2011/04/07/guenter-krings-cdu-internetgemeinde-das-klingt-schon-nach-sekte/].

ARCHITEKTUR IN SICHERHEITSGESELLSCHAFTEN

SICHERHEITSARCHITEKTUR UND DER EINFLUSS AUF DAS TÄTERVERHALTEN AM BEISPIEL BANKRAUB

Birgit Zetinigg, B.A., MSc

Dieser Artikel erörtert den Einfluss der Sicherheitsarchitektur auf das Tatverhalten von verurteilten Bankräubern. Täterbefragungen ergaben, dass die Gestaltung der Bankfilialen ausschlaggebend für die Objektwahl und die Durchführung der Tat ist.

1 Kriminalprävention und die bebaute Umgebung

Man geht mittlerweile davon aus, dass die Form und die Gestaltung der bebauten Umgebung einen großen Einfluss auf die Gelegenheit eine Straftat zu begehen, haben. Ein erheblicher Prozentsatz an Kriminalität findet an bestimmten Orten statt. Die Charakteristika dieser Orte in Bezug auf ihr generelles Setting, als auch auf ihre zusätzlichen Eigenschaften wie zum Beispiel planerische Gestaltungselemente, beeinflussen die Kriminalitätsformen die dort stattfinden (oder auch nicht stattfinden).

2 Design der Studie "Bankraub in Österreich"

Die Studie "Bankraub in Österreich" [1] wurde von fünf Banken in Auftrag gegeben, mit dem Ansinnen Daten zu generieren, die Licht auf das Täterverhalten und deren Auswahlkriterien werfen. In der Studie wurde im Speziellen der Zusammenhang von subjektiven und situativen Aspekten bei der Auswahl von Bankfilialen für einen Bankraub untersucht. Dabei standen folgende Fragen im Mittelpunkt der Untersuchung: warum werden manche Filialen häufiger viktimisiert als andere und manche gar nicht? Warum wählen Täter eine ganz bestimmte Filiale aus, oft auch in einem Gebiet wo es eine große Dichte an Banken gibt? Welche Faktoren bzw. welche Charakteristika einer Bank sind für den Täter handlungsleitend bei der Objektwahl? Und schließlich, wie ist die Entscheidung einen Bankraub zu begehen in den Alltag eingebettet bzw. welche Entscheidungsprozesse werden dabei in Gang gesetzt?

Im ersten Schritt wurde in einer quantitativen Raumanalyse untersucht, welche Gemeinsamkeiten Bankobjekte aufweisen, die für einen Banküberfall ausgewählt wurden und was die Bedingungen für eine Viktimisierung sind.

Im zweiten Schritt wurden qualitative leitfadenunterstützte Interviews mit 41 inhaftierten Bankräubern durchgeführt. Die Stichprobe umfasste 40% aller (zu dem Zeitpunkt des Interviewprozesses von Mai bis Juli 2007) inhaftierten Bankräuber [2]. Dabei wurde der Fokus auf die Entscheidungsprozesse der Täter und die Einflussfaktoren bei der Objektwahl gelegt. Welche räumliche Faktoren der Banken und welche situativen Gegebenheiten waren zum Tatzeitpunkt entscheidend? Das heißt, was sind anziehende und was sind abschreckende Faktoren für den Täter? Und worin unterscheiden sich viktimisierte Banken von nicht viktimisierten Banken?

3 Tätertypen

Basierend auf Täterinterviews (n=41), die im Rahmen der zitierten Studie [3] und in Anlehnung an kriminologische Literatur wurden Tätertypen anhand von folgenden Kriterien definiert: Anzahl der Überfälle, Anzahl der Komplizen, Grad der Planung, Waffengebrauch, emotionaler Zustand während der Tat, Gewaltbereitschaft, Auswahlstrategie der Objekte, kriminelle Vorgeschichte und Art der Überführung. Bei der Verteilung der Tätertypen hat sich gezeigt, dass ein geringer Teil, nämlich nur 14,4 Prozent auf die Gruppe der Profis anfällt. 30,6 Prozent der Täter lassen sich der Gruppe der Amateure zuteilen und 55 Prozent der Gruppe der Intermediates [4]. Der typische Bankräuber widerspricht daher der gängigen Annahme, dass es sich hierbei um einen professionellen Täter handelt.

Bei der Objektwahl konnten Unterschiede zwischen den Tätertypen erkannt werden. Der Amateur ist ein Einzeltäter. Er hat keine kriminelle Vordelikte, dass heißt er ist unbescholten und noch nie mit dem Gesetz in Kontakt gekommen. Meist handelt er aus einer unmittelbaren finanziellen Notsituation heraus. Oftmals sind es Kreditschulden, Spielschulden oder auch privater Konkurs, die den Täter in diese Notlage bringen. Dementsprechend amateurhaft ist auch seine Vorgehensweise. Der Grad der Planung und Organisation ist sehr niedrig bis gar nicht vorhanden. Der Entschluss einen Bankraub zu begehen, entsteht daher oftmals sehr spontan. Er wählt die Objekte in seinem Lebensradius aus, das heißt meist kennt er die Bank schon, weil er dort Kunde ist oder er fährt tagtäglich an ihr vorbei am Weg zur Arbeit oder zur Stammkneipe. Der Amateur bevorzugt kleine Filialen mit möglichst wenig anwesenden Personen (Kunden, Mitarbeiter), da er auf Grund seiner Unerfahrenheit über eine geringe Situationskontrolle verfügt und hauptsächlich Attrappen oder auch Spielzeugpistolen als Waffe verwendet.

Der Intermediate hat schon eine kriminelle Vorgeschichte, es werden auch andere Eigentumsdelikte begangen bzw. auch Trafiken, Tankstellen und Wettbüros ausgeraubt. Dieser Täter ist daher schon erfahrener im Vergleich zum Amateur und hat schon einen vernünftigen Planungsgrad. Dieser Täter geht häufiger mit Komplizen vor, deren Organisation durch eine Rollenaufteilung geregelt wird.

Durch diese Rollenaufteilung erhöhen sie das Maß ihrer Situationskontrolle und können somit auch größere Banken mit mehreren anwesenden Personen überfallen. Dieser Tätertyp verwendet im Gegensatz zum Amateur meist scharfe Waffen.

Der Profi ist ein persistenter Bankräuber. Er zeichnet sich durch seine äußerst rationale und elaborierte Tatplanung und Organisation aus. Er plant schon im Vorhinein Hindernisse (Videoüberwachung, Alarmpaket, Türen, Polizei, Kunden…) mit ein und überlegt sich eine Taktik, wie er mit diesen umgehen könnte. Der Profi verfügt durch seine kriminelle Vorerfahrung über eine hohe Situationskontrolle und kann daher sowohl mit Komplizen, als auch alleine vorgehen. Seine bevorzugte Objektwahl ist unabhängig von der Anzahl der anwesenden Personen und der Größe der Bank. Der Profi ist durchaus Gewalt bereit und verwendet meist scharfe Waffen.

4 Diskrepanz zwischen Sicherheit und Kundenfreundlichkeit

Eine Bank ist wahrscheinlich der öffentliche Ort mit einer der meisten Sicherheitsvorkehrungen. Es stellt eine große Herausforderung dar, Sicherheit zu gewährleisten und zugleich eine kundenfreundliche Atmosphäre zu schaffen. Auf der einen Seite werden Banken dazu angehalten ihre Sicherheitsvorkehrungen zu erhöhen, um erstens Geld und andere Wertsachen in der Bank zu schützen und zweitens um für die Sicherheit von Kunden und auch von Bankangestellten zu garantieren. Auf der anderen Seite sehen sich die Banken aus kommerziellen Gründen dazu gezwungen ihre Sicherheitsmaßnahmen zu reduzieren, um eine möglichst kundenfreundliche Atmosphäre zu schaffen. Daher ging der Trend hin zu einer offenen und frei zugänglichen Schaltergestaltung, um möglichst alle Barrieren zwischen dem Kunden und den Bankangestellten zu reduzieren. Die Kassa wurde meist nahe der Eingangstüre platziert, damit der Kunde möglichst wenig Weg zurücklegen musste, um zur Kassa zu gelangen. Sicherheitsrelevante Aspekte rückten somit oft in den Hintergrund und mussten marketingwirksamen Strategien weichen. Man könnte behaupten, dass der Grad der Sicherung einer Bank das Resultat dieses Dilemmas ist. Mittlerweile ist der Trend jedoch wieder rückläufig und von einer offenen, frei zugänglichen Kassengestaltung wird wieder abgegangen.

5 Auswahl und Beurteilung der Tatobjekte durch die Täter

5.1 Größe des Foyers

Bei der Untersuchung wurde von der Überlegung ausgegangen, dass Filialen mit kleinen Foyers häufiger Opfer von Überfallen werden. Tatsächlich besteht ein signifikanter Zusammenhang zwischen der Größe des Bankfoyers und der Viktimisierungswahrscheinlichkeit:

Je kleiner ein Bankfoyer ist, desto höher ist die Wahrscheinlichkeit einer Viktimisierung: 68% der Filialen, die ein kleines Foyer mit bis zu 20m² aufweisen, wurden Opfer eines Bankraubs. Bei großen Eingangsbereichen mit mehr als 48m² war die Viktimisierungsrate um 24% geringer. Bereits Wise and Wise [5] fanden den negativen Zusammenhang zwischen Foyergröße und Viktimisierung in ihrer Studie bestätigt.

5.2. Lage und Aufbau der Kassa

Bei einem Banküberfall ist Zeit ein ganz entscheidender Faktor für den Täter. Je mehr Zeit während der Überfallshandlung vergeht, desto größer ist die Chance die Kontrolle über die Situation zu verlieren und auch die Gefahr gefasst zu werden steigt erheblich. Durchschnittlich setzen sich die Bankräuber ein Zeitlimit von circa zwei Minuten für den Überfall. Überfälle, die dieses Zeitlimit überschreiten, stellen ein potentielles Risiko für den Täter dar. Zwischenfälle können jederzeit passieren, neue Kunden können die Bank betreten, anwesende Personen können in Panik unberechenbar handeln und die Exekutive könnte am Tatort sein bevor der Täter die Flucht ergreifen kann. Der Täter ist sich dessen bewusst und wird versuchen möglichst schnell die Überfallshandlung durchzuführen und auch seinen Aktionsradius möglichst klein zu halten. Je größer der „bedrohte“ Raum ist, desto schwieriger ist es, besonders als Einzeltäter, die Situation unter Kontrolle zu behalten. Ab dem Betreten der Bank befindet sich der Täter in einer Bedrohungssituation, nicht nur er bedroht, sondern auch er wird bedroht. Es kann jederzeit etwas Unvorhergesehenes passieren, was ein Täter vorher kaum einkalkulieren kann. Die psychologische Barriere beim Betreten der Bank ist immens und ein Täter weiß, sobald er die Tür öffnet, gibt es kaum ein Zurück. In dieser Hinsicht ist es für viele Täter auch angenehmer, wenn der bedrohte Bereich den sie durchschreiten müssen klein ist. Je schneller ein Täter aus der Bank wieder herauskommt, desto besser ist es für ihn. Interviews mit inhaftierten Bankräubern bestätigten die schon vorhin erwähnte Hypothese, dass ein kleines Foyer und ein kurzer Weg zur Kassa für die Täter durchaus günstig sind. Aufgrund ihrer geringen Situationskontrolle bevorzugen besonders Amateure kleine Filialen, die möglichst übersichtlich sind.

> *Interviewer (I): Und die Kasse war die ganz beim Eingang oder war die weiter hinten?*
>
> *Siegfried (S): Ah, warte einmal, Eingang ist links, also, ziemlich nah am Eingang, weil direkt der erste Schalter, doch näher beim Eingang...*
>
> *I: War das gut für sie oder war das eher schlecht*
>
> *S: Ja eigentlich schon also, je näher desto besser sage ich einmal. Weil im Endeffekt jede Sekunde zählt (Siegfried).*

Ein weiterer für Bankräuber förderlicher Aspekt der Kassa ist nicht nur deren geringe Distanz zum Eingang, sondern auch die offene und von allen Seiten zugängliche Bauweise.

Albert (A): Nein waren eigentlich alle sehr übersichtlich.

Interviewer (I): War das auch angenehm für Sie?

A: Schon ja.

I: Schon, dass man alles unter Kontrolle hat?

A: Man hat zumindest das Gefühl, dass man das unter Kontrolle hat...zum Beispiel ist dort hinten ein Aufenthaltsraum, wo vielleicht zwei Leute rauskommen...(Albert)

Eine Kassa in Nähe des Ausgangs in Kombination mit einer offenen Kassengestaltung ist für viele Täter eine günstige bauliche Bankgestaltung. Je näher die Kassa beim Eingang platziert ist, desto schneller kann der Täter den Tatort auch wieder verlassen, da er weniger Zeit verliert und sich ihm weniger Hindernisse in den Weg stellen können. Außerdem ist eine offene, von mehreren Seiten zugängliche Kassa für den Täter förderlich, da er sich selbst bedienen kann und keine physische und auch symbolische Barriere überwinden muss. Sobald der Bankangestellte der Forderung des Täters nachkommt, kann der Täter sich selbst an der Geldlade bedienen und ist nicht auf die Geldausgabe der Angestellten angewiesen. Das heißt, der Täter kann das Tempo selbst regulieren und muss nicht mit Zwischenfällen bei der Geldausgabe rechnen, wie zum Beispiel mit geschockten und folglich langsam agierenden Angestellten. Der Bankangestellte hat ja darüber hinaus die Direktive, in jedem Falle mit dem Bankräuber kooperieren zu müssen. Dieses Wissen macht es auch für Täter mit geringer Situationskontrolle möglich, den Überfall erfolgreich durchführen zu können. Damit wird die zu überwindende Schwelle sehr niedrig und das Geld scheint gleichsam „zum Greifen nahe“.

Adam (A): Und ich hab halt dann wirklich erkannt, dass ich eben viel schneller bin, wenn ich selbst hinten rum geh und da nicht dem Kassier sag: Geld raus.

Interviewer (I): Ja. Ja. Ja.

A: Und der hat dann alle Zeit der Welt und ist vielleicht noch durch das Glas geschützt und ja.

I: Wo die Kasse ist, was würde das für einen Einfluss haben? Nicht zu wissen.

A: Naja, weil dort steht die Kassa fast in der Mitte von der Bank, also kann man leicht dahinter, aber bei manchen Banken, viel neueren Banken, haben sie da schon so eine Plexiglasscheibe. Und da kann man nicht hinter die Kassa, man kann nicht schauen wie viel Geld drinnen ist und so...(Adam).

Otto: Das Geld ist so nah. Weil man – weil's öffentlich ist, nicht. Das Ganze. Das ist alles so öffentlich. (Otto)

Man kann feststellen, dass es einen Konflikt zwischen einer für Kunden barrierefreien, offenen Bauweise der Kassa und einer geschlossenen, dafür sicheren Gestaltung gibt. Die gängige Annahme ist, dass Kunden eher eine offene, frei zugängliche Innengestaltung einer Bank bevorzugen und sie sich so eher in einer Atmosphäre befinden, die sich günstig auf deren Konsumverhalten auswirkt. Auf der anderen Seite schafft diese offene Gestaltung ein durchaus Kriminalität förderndes Umfeld durch die für den Täter fehlende Barriere.

5.3 Beschaffenheit der Eingangstür

Für einen Bankräuber ist es essentiell, die Bank möglichst schnell und ohne Zwischenfälle nach der Tat verlassen zu können. Jede noch so kleine Zeitverzögerung könnte zu einer Festnahme beitragen. Daher ist es für den Bankräuber nicht nur wichtig zu wissen, wie er in die Bank hineinkommt, sondern auch wie er, möglichst ohne Zwischenfälle, wieder schnell herauskommt. Die Tür ist hier das entscheidende Kriterium. Die größte Sorge eines Bankräubers ist in der Bank oder im Foyer gefangen zu werden. Dann kann nämlich genau das passieren, was die meisten Bankräuber scheuen. Es kann zu einer Eskalation kommen, die womöglich nur mit Gewalt beendet werden kann.

Bei den Interviews wurde festgestellt, dass die Beschaffenheit der Eingangstür für einen Teil der Täter, nämlich 14 von 37, ein Kriterium darstellt, worüber sie sich vor dem Banküberfall Gedanken machen oder das sie in ihrer Handlungsweise beeinflusst.

> *„I (Interviewer):Und mich interessiert es trotzdem noch immer, wie Sie das geplant haben - diese Objektauswahl. Was war für Sie wichtig?*
>
> *Stefan (S): Ja es war für mich wichtig, dass die Türen sehr gut waren.*
>
> *I: Was heißt das?*
>
> *S: Dass der Eingang nicht irgendwie technisch - so durch eine Funktion verschlossen werden kann, wo sie nicht mehr aufgeht dann.*
>
> *I: Ja. Okay, dass es keine technischen Maßnahmen gibt, die die Türen zumachen.*
>
> *S: Ja und es gibt auch so Pendeltüren und dann die erste tsch tsch dann gehst du und dann kommt die nächste und das ist der Leerraum. Und da könnten sie dich fangen.“ (Stefan)*

Eine elektrische Tür wird hier als Risiko angesehen, das die Situationskontrolle für den Täter erschwert. Elektrische Türen haben durchaus eine abschreckende Wirkung auf Bankräuber, da sie als Barriere gesehen werden, die der Täter psychisch, aber auch physisch überwinden muss.

5.4 Transparenz der Filiale

Die Transparenz beziehungsweise die Einsehbarkeit in eine Filiale, wurde als bauliche Maßnahme eingesetzt um einerseits eine Filiale für Kunden attraktiver und freundlicher zu gestalten, aber auch, um etwaige Bankräuber abzuschrecken. Die Transparenz sollte einen potentiellen Täter suggerieren, dass er jederzeit von außen beobachtbar ist und im Falle eines Überfalls mit Interventionen zu rechnen habe. Diese Überlegung entsteht aus dem Prinzip der "natürlichen Überwachung"[6]. Hintergrund dieses Konzeptes ist, dass dem täglichen Benutzer durch spezielle Architektur und Design ermöglicht wird, den Raum (besonders gefährdete Räume) ohne Hindernisse zu überblicken und einsehen zu können. Dadurch entsteht eine natürliche Überwachung des Raums durch den Benutzer, was potentielle Täter wiederum abschrecken sollte.

Die Interviews mit Bankräubern zeigten, dass diese bauliche Gestaltung sowohl positive, das heißt für die Tat förderliche, als auch negative beziehungsweise abschreckende Aspekte darstellte.

5.4.1 Günstig für den Täter

Die Transparenz kann sich zu Gunsten der Bankräuber auswirken in dem Sinn, dass der Täter zum Ausspionieren nicht mehr die Bank betreten muss. Der Täter braucht die Bank vor dem Überfall nicht mehr betreten, um an Informationen, wie zum Beispiel den Weg zur Kassa, die Anzahl der Kassenschalter, Aufbau der Innenräume usw., heranzukommen. Dadurch verringert sich für den Täter die Chance von einer Überwachungskamera aufgenommen und nach dem Überfall anhand der Videoaufnahmen erkannt zu werden. Aber auch unmittelbar vor einem Überfall beim Zugang zur Bank kann die Transparenz dazu genutzt werden, um die Kundenfrequenz und die Anzahl der Bediensteten schnell zu überprüfen. Besonders die Anzahl der Kunden in einer Filiale ist ein wichtiges Kriterium für einen Großteil der Täter. Noch mehr für Täter, die ohne Komplizen vorgehen, ist es wichtig die Situation und die anwesenden Menschen unter Kontrolle zu haben. 61,1% der Täter gaben an, dass sie wenige bis keine Kunden bevorzugen und mit dem Betreten der Bank warten, wenn sich zu viele Kunden in der Bank aufhalten. Im Gegensatz zu der Anzahl der Bankangestellten, kann der Täter durchaus die Anzahl der Kunden bis zu einem gewissen Grad beeinflussen, indem er einfach abwartet, bis wenig Kunden in der Filiale sind. Daher ist auch die Transparenz für einen Großteil der Täter, nämlich 57,1% ein sehr positiver baulicher Effekt.

Täter nützen die Transparenz oftmals dazu, um einen günstigen Moment abzuwarten, in dem sich möglichst wenige Kunden in der Bank befinden. Der Täter kann durch die einsichtige Gestaltung relativ einfach und unauffällig die Kundenfrequenz beobachten und muss nur auf den „richtigen“ Moment warten. Besonders Täter der Gruppe der Amateure, die sich durch ihre geringe Situationskontrolle kennzeichnen, verwenden die Transparenz dazu um mehr Situationskontrolle zu erlangen.

Dieser Täter wartet zum Beispiel so lange bis sich keine Kunden in der Bank befinden, um dann den Überfall zu initiieren.

> *Interviewer (I): Dann sind sie hingefahren und haben sie vorher geschaut…*
>
> *Siegfried (S): Ja, ich bin hingefahren und habe das Fahrrad hinter der Bank deponiert gehabt und bin dann glaube ich, ich weiß nicht, sicher 10, 12 Mal um den Block, weil ich mich nicht hineingetraut habe und irgendwann ist mir die Situation dann ziemlich günstig vorgekommen und...also ich habe nicht keinen Kunden drinnen gesehen, es war noch eine Dame drinnen, die sich angestellt hat bei der Kassa gerade und ja habe dann...die Handschuhe habe ich angezogen und die Softgun habe ich auch gezogen und bin hineinmaschiert. Ja und habe eben Geld gefordert." (Siegfried)*

Einige Täter sehen den fehlenden Abschreckungseffekt der Transparenz im Desinteresse und in der mangelnden Zivilcourage der Menschen. Auch wenn der Überfall als solches von außen erkannt werden würde, zweifeln die Täter an einer Intervention der vorbeigehenden Passanten.

> *Interviewer (I): Und wenn so transparente - Glas - wenn man draußen steht oder wie ist das wenn man dann drinnen ist als Bankräuber, ist das dann unangenehm - diese Transparenz zum Beispiel?*
>
> *Albert (A): Eigentlich nicht. Muss ich ehrlich sagen.*
>
> *I: Also ist das Positive überwiegend da?*
>
> *A: Weil im Regelfall krieg ich ja die Bank gemacht - weil den Leuten oder selbst wenn da vielleicht irgendwer hereinschauen würde, ja - es ist ihnen im Prinzip egal. Es macht keiner was. Das ist irgendwo vielleicht ein Phänomen der heutigen Zeit, aber es ist so. Es ist genauso, was weiß ich - eine Schlägerei in der U-Bahn. Es dreht sich jeder weg. Da schaut keiner, sollte ich dem vielleicht helfen oder so. Du rufst nicht mal die Polizei an. Das ist wurscht. Also. (Albert)*

Die Transparenz kann für den Täter auch während des Überfalls dienlich sein, wenn der Täter sich in der Bank befindet. Der Täter kann dadurch sehen, was ihn vor der Bank erwartet, zum Beispiel ob eine Polizeistreife am Tatort vorbei fährt. Dadurch kann sich der Täter besser darauf einstellen, wie er sich zu verhalten hat und wie seine Flucht erfolgen muss.

5.4.2 Ungünstig für den Täter

Die Transparenz kann sich jedoch auch negativ gestalten, dadurch dass der Täter quasi in einem „Schaufenster" den Überfall begeht und damit rechnen muss, dass er von außen beobachtet wird. Frühzeitiger Alarm verkürzt die Zeit, welche die Polizei zur Intervention benötigt. 17,1% der Täter gaben an, dass eine transparente Bank negativ für sie sei, da sie sich beobachtet fühlen würden.

Stefan (S): Und das sind so Kriterien. Wenn eine Bank natürlich eine einzige Glasfront ist und man sieht von der Straße schon in den Schalter rein, dann ist das mit Vorsicht zu genießen.

Interviewer (I): Für Sie mit Vorsicht? Also für Sie ist das nicht so gut meinen'S jetzt.

S: Nein. (Stefan).

Es gab aber auch Täter (11,4%), die die Transparenz sowohl als positiv (zum Auskundschaften) als auch als negativ (Schaufenstersituation) empfinden. Das heißt die Transparenz hatte einen durchaus zwiespältigen Effekt auf einige Täter. 14,3% der Täter gaben an, auf die transparente Beschaffenheit der Bank entweder nicht geachtet zu haben, oder dieses als nicht relevantes Kriterium zu sehen.

6 Fazit

Der Gedanke, die Sicht des Täters (Denkweise, Vorerfahrung, Modus operandi...) im Rahmen der Kriminalprävention nutzbar zu machen, stellt in vieler Hinsicht eine vielversprechende Vorgehensweise dar. Bislang fehlte diese "Kundenbefragung" besonders am österreichischen Parkett und im Speziellen noch, wenn man die Deliktsform des Bankraubes betrachtet. Zunächst musste man auf Erfahrungen der Exekutive zurückgreifen, die diese aus bereits schon bearbeiteten Fällen generiert. Schwind und Steinhilper [7] gehen "davon unausgesprochen aus, dass der Täter das Mißerfolgsrisiko (bzw. Entdeckungsrisiko) für seine Tat etwa so einschätzt wie die Polizei selbst". Jedoch diese Annahmen müssen nicht stimmen, da es von Dritten schwer nachzuvollziehen ist, welche Umstände den Täter dazu bewogen haben und bewegen, ganz spezielle Objekte auszuwählen und andere außer Acht zu lassen. Die situative Kriminalprävention beruht daher weitgehend auf Spekulationen (etwa, dass Täter vermeiden "defensible space" zu betreten) oder auf gesundem Menschenverstand (etwa, dass ein Sicherheitsschloss das Eigentum schützen kann) [8]. Umso wichtiger sind die Einblicke, die einem Täterbefragungen ermöglichen. Täterbefragungen mit 40 inhaftierten Bankräubern, die im Rahmen der Studie "Bankraub in Österreich" [9] durchgeführt wurden, ergaben, dass die Gestaltung von Bankfilialen auf die Objektwahl und dem Modus Operandi der Täter einen Einfluss hat. So können bestimmte gestalterische Elemente auf den Täter abschreckend oder auch anziehend wirken. Wie die Interviews gezeigt haben, lassen sich Täter durchaus von situativen und/oder baulichen Maßnahmen abschrecken bzw. kann dadurch die Begehung des Delikts Bankraub erheblich erschwert werden. Besonders Amateure mit einer nicht sonderlich elaborierten Vorgangsweise lassen sich bereits durch relativ einfache Mittel verunsichern und in weiterer Folge vielleicht sogar abhalten, einen Raub zu begehen. Der Handlungsdruck, unter dem sie stehen lässt eine komplexe Planung kaum zu.

Gewisse bauliche Maßnahmen sind jedoch notwendig, um den Tätern ein "kriminalitätsfeindliches" Umfeld zu gestalten.

Eine Kassa in Nähe des Ausgangs ist für viele Täter eine günstige bauliche Bankgestaltung. Je näher die Kassa beim Eingang platziert ist, desto schneller kann der Täter den Tatort auch wieder verlassen, da er weniger Zeit verliert und sich ihm weniger Hindernisse in den Weg stellen können. Ein nicht zu unterschätzender Teil der Täter gab ebenso an, dass ihnen durch die freie und offene Gestaltung des Kassenbereiches die Tatbegehung erheblich erleichtert werde. Diese offene Bauweise erzeugt ein Kriminalität förderndes Umfeld und suggeriert so dem Täter, er befinde sich in einem „Selbstbedienungsladen“. Der Täter erfährt so weder eine physische, noch eine psychologische Barriere.

Elektrische Türen haben wiederum eine durchaus abschreckende Wirkung auf Bankräuber. Immerhin 14 von 37 Tätern erwähnten die Beschaffenheit der Eingangstür als ein Element, das ihre Handlungsweise beeinflusst. Eine zeitverzögerte Öffnung der Türen könnte den Tätern die Flucht verlangsamen und somit wichtige Zeit kosten. Eine elektrische Tür wird als Risiko angesehen, das die Situationskontrolle für die Täter erschwert.

Die Transparenz einer Filiale scheint auf doch mehr als die Hälfte der Täter, nämlich 57,1% einen positiven Effekt zu haben. Täter verwenden die Transparenz, um die Banken auszukundschaften, aber auch um kurz vor der Tat die Kundenfrequenz zu kontrollieren. Dem gegenüber stehen 17,1% der Täter, die definitiv angeben, dass sie eine transparente Bank abschreckt.14, 3% der Bankräuber scheint die Transparenz komplett gleichgültig zu sein.

Literatur

[1] ZETINIGG, B. und GADERER, M., Projektendbericht, Bankraub in Österreich: Subjektive und situative Aspekte der (Re-) Viktimisierung von Bankfilialen, Wien, 2007

[2] ZETINIGG, B.and GADERER, M., Validating offenders'accounts: learning from offender interviews with bank robbers in Austrian prisons, in: BERNASCO, W.(ed.), Offenders on Offending, Devon, 2010.

[3] ZETINIGG, B. und GADERER, M., Projektendbericht, Bankraub in Österreich: Subjektive und situative Aspekte der (Re-) Viktimisierung von Bankfilialen, Wien, 2007.

[4] ZETINIGG, B., Workshop: Analyse von Tätertypen und situativen Gegebenheiten im Bankenbereich, Wien, 2008

[5] WISE, J.A. and WISE, B.K..: Bank Interiors and Bank Robberies: A Design Approach to Environmental Security, Bank Administration Institute, Illinois, 1984.

[6] SCHNEIDER, R.H. and KITCHEN, T., Crime Prevention and the Built Environment, London, 2007.

[7] SCHWIND, H.D., Kriminologie: Eine praxisorientierte Einführung mit Beispielen, S 333.Heidelberg, 2004.

[8] BENNETT, T. and WRIGHT, R., Offender-Perceptions of Targets, in: Research Bulletin (Hmoe Office), London, 1983

[9] ZETINIGG, B. und GADERER, M., Projektendbericht, Bankraub in Österreich: Subjektive und situative Aspekte der (Re-) Viktimisierung von Bankfilialen, Wien, 2007

Weiterführende Literatur:

AUSTIN, C. The Prevention of Robbery at Building Society Branches. Crime Prevention Unit: Paper 14, Home Office, London, 1988.

BURKE, R., H., An Introduction to Criminological Theory, Devon 2001

CANTER, D. and ALISON L. (ed.), The Social Psychology of Crime: Groups, Teams and Networks,Aldershot, 2000.

CANTER, D. and ALISON L., Profiling Property Crimes, Aldershot, 2000.

CSASZAR, F., Der Überfall auf Geldinstitute: Eine kriminologische Untersuchung, Wien,1975.

CROMWELL, P., In their own Words: Criminals on Crime. An Anthology (4th edn), Los Angeles, 2006.

EUROPEAN BANKING FEDERATION, Bank Robberies & Other Bank Raids (14th Report). European Banking Federation, Brussels, 2006.

DESROCHES, F.J., Force + Fear: Robbery in Canada, Toronto, 2002.

KATZ, J. Seductions of Crime: Moral and Sensual Attractions in Doing Evil. U.S., 1988.

MATTHEWS, R., Armed Robbery, Cullompton, 2002.

MATTHEWS, R., PEASE, C. and PEASE, K., Repeated Bank Robbery: Theme and Variations. Crime Prevention Studies, volume 12, pp. 153-164

SCHÖNBERGER, K., Vabanque. Bankraub, Theorie, Praxis, Geschichte, Berlin, Hamburg, Göttingen, 2001.

SERVAY, W. und REHM, J., Bankraub aus Sicht der Täter. BKA-Forschungsreihe, Band 19, Wiesbaden, 1986.

SHERMAN, L.,W. et. al, Evidence-Based Crime Prevention, Abingdon, 2006.

TILLEY, N., Handbook of Crime Prevention and Community Safety, Devon, 2005.

DIE MORPHOLOGIE DER SICHERHEITSGESELLSCHAFT: ARCHITEKTONISCHE ANTWORTEN IN DER KRIMINOLOGIE

Dr. Günter Stummvoll

In diesem Beitrag wird über gegenwärtige Gesellschaftsentwicklungen nachgedacht. Die Sicherheitsgesellschaft steht als Synonym für den aktuellen Umgang mit Kriminalität und Unsicherheit. Sie äußert sich in Präventionsmaßnahmen, die oft erst auf den zweiten Blick ins Auge springen, weil sie so selbstverständlich geworden sind, dass man die Wirkungen und Konsequenzen nicht wahrnimmt. Die These lautet: Die Maximen der Sicherheitsgesellschaft lassen sich in der architektonischen Gestaltung unserer Umwelt ablesen. Dazu ist zunächst zu klären, was unter dem Begriff „Sicherheitsgesellschaft" zu verstehen ist, um danach den Nachweis zu erbringen. Zur Beschreibung und Erklärung gesellschaftlicher Entwicklungen auf dem Gebiet der Sicherheit wurde die spezielle Methode der Sozialen Morphologie aus dem soziologischen Repertoire entlehnt, um das materielle Substrat sozialer Gegebenheiten in der Umwelt nachzuzeichnen.

Schlagworte: Sicherheitsgesellschaft, Soziale Morphologie, Architektur, Städtebau, Defensive Design, Raumpsychologie, Sozialraummanagement

1 Kriminologie: Sicherheit - Gesellschaft

In Österreich wird Kriminologie als akademisches Fach auf juridischen Fakultäten gelehrt. Damit wird nahegelegt, dass die „Lehre von der Kriminalität" eine Angelegenheit der Rechtswissenschaften sei, und folglich die Justiz damit zu befassen ist (Kunz 2008). Die Kriminologie ist zum einen eng verwandt mit der Strafrechtswissenschaft, obwohl sich diese mit den Voraussetzungen unter denen Strafe verhängt und vollstreckt werden darf befasst, während sich die Kriminologie mit der Kriminalitätswirklichkeit in der Gesellschaft beschäftigt. Zum zweiten ist die Kriminologie auch mit der Kriminalistik verwandt, die sich allerdings als Hilfswissenschaft der Strafverfolgung mit der fallbezogenen Aufdeckung von Straftaten befasst. Die Kriminologie ist dagegen eine *Bezugswissenschaft*, die Relationen zu besonderen Wissensgebieten herstellt:

Kriminal*soziologie*, Kriminal*psychologie*, Kriminal*biologie*, Kriminal*politik* und dergleichen.

KriminologInnen sind somit thematisch relativ frei, sie können Ausflüge machen und sozusagen in fremden Gewässern fischen, solange sie sich mit deviantem Verhalten befassen. Die kritische Distanz zum Kriminaljustizsystem mit seinen Institutionen der Legislative, Exekutive, Judikatur und den Einrichtungen im Strafvollzug eröffnet dabei neue Perspektiven auf das Phänomen Kriminalität, und insbesondere auf den gesellschaftlichen Umgang mit deviantem Verhalten. Der Nachteil ist allerdings, dass kriminologische Diskurse oftmals auf einzelne Themen beschränkt sind, also entweder bestimmte Kriminalitätsformen in den Blick fassen (Drogenkriminalität, Gewaltkriminalität, Wirtschaftskriminalität, etc.) und dabei bestimmte Ideologien verfolgen. Beispielsweise verfolgen viele KriminologInnen, die ihre akademische Heimat vor allem in der Soziologie haben, ein eher liberales Paradigma, sie interessieren sich für Kriminalität im Hinblick auf soziale Ungleichheit und Ungerechtigkeit in der Gesellschaft, was jedoch gleichzeitig den kritischen Blick auf gesellschaftspolitische Tatsachen schärft. KriminalpsychologInnen befassen sich gerne mit einer Systematisierung von Persönlichkeitsmerkmalen von Tätern und erstellen Täterprofile. Die forensische Psychiatrie interessiert sich für die Schuldfähigkeit und die Einschätzung der Gefährlichkeit von Straftätern sowie deren Behandlung. Während sich also Psychologie und Psychiatrie in erster Linie mit dem Verhalten von Tätern (oder Opfern) auseinander setzen, geht es der Soziologie um Kriminalität als gesellschaftliches Phänomen, und dabei werden Entwicklungen gerne in historischen Vergleichen betrachtet: Wie haben sich Häufigkeiten von Gewalt, Diebstahl, Einbruch, Drogenhandel entwickelt? Welche neuen Formen der Kriminalität sind in den Vordergrund getreten (Cybercrime, Stalking, organisierte Kriminalität)? Haben sich Sanktionen verändert (Vergeltung, Strafen, außergerichtliche Verfahren)?

Welche Herausforderungen sind dadurch für justizielle Institutionen entstanden, und wie gehen diese damit um? Der amerikanische Kriminologe Edwin Sutherland hat es bereits in den 1930er Jahren auf den Punkt gebracht. Die Kriminologie versucht folglich drei Fragen zu klären: Wie werden Gesetze gemacht? Wie werden Gesetze gebrochen? Und welche Konsequenzen hat eine Gesetzesverletzung für den Täter aber auch für die Gesellschaft? Der Beschäftigung mit diesen Fragen wurden andere hinzugefügt, die sich mit Kontroll- und Ordnungs*politiken* befassen, dabei über ausschließlich juristische Tatsachen hinausgehen, und allgemeine Ordnungskonstruktionen und Abweichungen von gesellschaftlichen Normen behandeln. Diese und andere Fragen beschäftigen Kriminalsoziologen bis heute (vgl. Carrabine et al. 2004; Kunz 2008, Newburn 2007).

1.1 Kontrollkulturen

Einer der bedeutendsten Kriminalsoziologen der Gegenwart ist David Garland, Professor für Soziologie und Recht an der New York Universität.

In seinem einflussreichen Buch „Culture of Control“ (Garland, 2008; orig. 2001) entwirft Garland in der Tradition Michel Foucaults’ eine „Geschichte der Gegenwart“, und beschreibt gesellschaftlichen Wandel anhand eines radikalen Paradigmenwechsels in der Kriminalpolitik im Übergang zur Späten Moderne: Das „wohlfahrtsstaatliches Strafen“ der Nachkriegszeit, mit dem Ziel der Besserung von Straftätern, Resozialisierung und Re-Integration in die Gesellschaft, wird sukzessive verdrängt durch ein neues Bild sozialer Kontrolle. Vorbeugende Maßnahmen, in der Form von Alarmanlagen, Videoüberwachung, Vorratsdatenspeicherung, Ausgangssperren für Asylwerber, verschärften Zugangskontrollen auf Flughäfen, biometrischen Kontrollen und Vieles mehr, werden eingesetzt, um soziales Verhalten zu kontrollieren und Risiken zu minimieren. Dazu bedient sich die Politik einer intelligenten Sicherheitstechnologie, die inzwischen sowohl in der Forschung und Entwicklung, als auch in der kommerziellen Anwendung zu einem bedeutenden Marktsegment geworden ist (Zinganel 2003). Neben dem Angebot von Sicherheitsprodukten zählt der Aufruf der Behörden zum Selbstschutz als wesentlicher Bestandteil der neuen staatlichen Präventionsstrategie:

Der Aufruf zu Eigenverantwortlichkeit und Eigeninvestition in Sicherheitstechnologie (Sicherheitstüren, Alarmsysteme, etc.) wird zum Credo der polizeilichen Präventionsarbeit.

Zu den kriminalpolitischen Veränderungstendenzen der letzten 30 Jahre zählt Garland eine Reihe von Merkmalen, die hier nur rudimentär wiedergegeben werden können:

- Der Niedergang des „rehabilitativen Ideals“ bei gleichzeitiger Radikalisierung strafrechtlicher Maßnahmen, die der populistischen Forderung nach Risikominimierung, sozialer Exklusion und Vergeltung folgen.
- Meinungsforschungen bestätigen die zunehmende Angst und Empörung in der Bevölkerung, und dieses Empfinden einer ängstlichen bis wütenden Öffentlichkeit hat den Stil und Inhalt der Politik in den letzten Jahren beeinflusst.
- Das allgemeine Täterbild hat sich verändert: „Das gängige wohlfahrtsstaatliche Bild vom Delinquenten als benachteiligtem, bedürftigen, aus der Not heraus handelnden Menschen ist fast völlig verschwunden (Garland 2008, S. 54)“. Stattdessen werden Verbrecher entweder als Psychopaten oder als Berufsverbrecher aus fremden Kulturen und anderen Ländern betrachtet.
- Das Gefängnis, das in seiner ursprünglichen Konzeption im 18. Jahrhundert lediglich als „Warteraum“ auf die Urteilsverkündung bzw. –vollstreckung gedacht war - vergleichbar mit der heutigen Untersuchungshaft, erlebte im 20. Jahrhundert einen Höhenflug.

Bei anhaltend hohen Gefangenenzahlen gilt das Gefängnis heute jedoch nicht mehr als „Besserungsanstalt“ oder als „Resozialisierungsmechanismus“, sondern als Mittel des Freiheitsentzugs und der Bestrafung, das die populistische Forderung nach Vergeltung befriedigt.

- Erklärungen für die Ursachen kriminellen Verhaltens erfahren einen Wandel von dem einst zentralen Erklärungsansatz der „sozialen Deprivation“, verursacht durch mangelnde Erziehung, fehlende Bildung, schlechte Arbeitsmarktchancen oder mangelnde Behandlung psychischer Störungen, hin zu verschiedensten Kontrolltheorien, also Erklärungen durch unzureichende soziale Kontrolle, polizeiliche Kontrolle oder Selbstkontrolle.
- Zu der Zeit als Kriminalität als Zeichen eines unzureichenden Sozialisierungsprozesses begriffen wurde, hat man Prävention als resozialisierende Behandlung verstanden, die auf Einzelne zugeschnitten war. „Während die ältere Kriminologie mehr Wohlfahrt und Unterstützung forderte, beharrt die neue auf verstärkten Kontrollen und der Durchsetzung von Disziplin (Garland 2008, S. 63)“.

Die kritische Auseinandersetzung mit dem Wandel der Kontrollkulturen in verschiedenen westlichen, demokratischen Gesellschaften hat auch in der deutschsprachigen Fachliteratur Eingang gefunden. Die Gedanken Garland’s zur aktuellen Kriminalpolitik werden unter dem Begriff „Sicherheitsgesellschaft“ zusammengefasst und erweitert.

1.2 Sicherheitsgesellschaft

Im Rahmen des 34. Kongresses der Deutschen Gesellschaft für Soziologie 2008 in Jena wurden „Wege der Sicherheitsgesellschaft“ diskutiert, und gemeinsam mit weiteren Beiträgen in einem Buch zusammen gefasst (Groenemeyer 2010). Groenemeyer konstatiert in seinem Einleitungsartikel einen Übergang von der Disziplinargesellschaft zur Sicherheitsgesellschaft. Die Disziplinargesellschaft war gekennzeichnet durch die Etablierung von „Interventionen, Dispositiven und Organisationen, mit denen die Anpassung der Individuen an die Erfordernisse der sozialen Ordnung gesichert werden sollten (ebd. S. 9)“. Der Disziplinargesellschaft ging es um die Disziplinierung und Reintegration von Tätern, oder wie Treiber und Steinert vor langer Zeit bereits treffend feststellten: Um die „Fabrikation des zuverlässigen Menschen“ (Treiber und Steinert, 1980). Die Sicherheitsgesellschaft ist dagegen gekennzeichnet durch die zentrale Bedeutung von Risiken und Unsicherheiten. Bei Aldo Legnaro, der den Begriff 1997 mit Bezug auf Ulrich Beck’s Perspektive der „Risikogesellschaft“ (1986) prägte, lautet eine Definition:

> *„Eine Sicherheitsgesellschaft zeichnet sich dadurch aus, dass nicht nur staatliche, sondern allmählich und in zunehmend stetigem Ausmaß auch private Akteure an der Produktion von Sicherheit teilnehmen, dass die Überwachung nicht nur dem Staatsschutz im engeren Sinne*

gilt, sondern Aktivitätskontrollen von allen Bürgern – tendenziell durch alle Bürger – mit dem Ziel der Risikominimierung für alle angestrebt werden und dass schließlich die Produktion von Sicherheit nicht nur eine staatliche Aufgabe ist, sondern eine permanente gesellschaftliche Anstrengung, ein Regime des täglichen sozialen Lebens (Legnaro 1997, S. 271 f.)".

In der Sicherheitsgesellschaft geht es nicht mehr um die Bestrafung von konkreten Regelverletzungen, sondern um das Management von Kriminalitätsrisiken, und darum alle Ungewissheiten kalkulierend in den Griff zu bekommen. Es geht um die rationale Antizipation von Risiken in der Zukunft, es geht um Prävention. Groenemeyer nennt sechs Entwicklungslinien zur näheren Charakterisierung der Sicherheitsgesellschaft (Groenemeyer 2010, S. 11 ff.):

- *Allgegenwärtigkeit von Bedrohungen der Sicherheit:* Eine Routinisierung von Sicherheit im Alltag der Menschen bedeutet nicht, dass plötzlich die Furcht vor Kriminalität ins Unermessliche steigt, sondern lediglich dass sich Menschen bestimmte Handlungen und Praktiken angewöhnt haben, um Risiken zu minimieren. Das Niveau der Risikominimierung mag in verschiedenen Städten unterschiedlich ausgeprägt sein, in Manchester höher als in Wien oder Graz, und in ländlichen Gemeinden vielleicht noch geringer sein. Klar ist jedoch, dass die Vorstellung von Risiken in einer Gesellschaft einer eigenen sozialen Konstruktionslogik folgt, die nicht zuletzt durch die Medien geprägt ist. Schließlich sind nicht nur die professionellen Risikomanager mit Risikokalkulation befasst, sondern gleichsam alle BürgerInnen einer Gesellschaft.
- *Entprofessionalisierung von Sicherheitspolitiken:* Kriminalitätskontrolle und Kriminalprävention war gerade in Kontinentaleuropa lange Zeit Aufgabe des Staates. Der Staat mit seinen Spezialisten der Exekutive, der Justizverwaltung und den sozialen Diensten war oberster Sicherheitsproduzent, während die BürgerInnen als Sicherheitskonsumenten galten. Zu Beginn des 21. Jahrhunderts ist der Staat im Begriff, sein Gewaltmonopol abzugeben und Aufgaben an andere Verwaltungseinrichtungen aber auch an zivilgesellschaftliche Organisationen abzutreten. Gleichzeitig werden Schulen, Sozialreinrichtungen, Jugendämter, Vereine, Banken, und Wirtschaftsbetriebe für kriminelle Taten haftbar gemacht, und sind für die Installation diverser Vorkehrungen zu Einhaltung von Sicherheitsbestimmungen selbst verantwortlich. Um aus der Not eine Tugend zu machen, wird die Allgegenwärtigkeit von Gefahren und Risiken strategisch genutzt, um mit Sicherheitsaspekten für seine Sache zu werben. Sicherheit wird zum Marketinginstrument.
- *Neukonfiguration öffentlicher Räume durch Privatisierung und Technisierung sozialer Kontrolle:* Öffentliches Leben verlagert sich zunehmend vom Straßenraum in geschlossene Räume der Einkaufszentren, der Kleinhandel der Einkaufsstraßen wird von breiten

Käuferschichten ignoriert, was zur Folge hat, dass die Erdgeschoßzone leer, verlassen und vernachlässigt wirkt und ganze Stadtteile ökonomisch verarmen. Das soziale Leben findet nun in den Entertainment-Centern am Stadtrand, oder neuerdings auch in Großbahnhöfen in Zentrumsnähe statt, wo allerdings private Betreiber erwünschtes Sozialverhalten in Hausordnungen festlegen und unerwünschtes Klientel ausschließen dürfen. Zur Kontrolle dieser neuen Legalverhaltensvorschriften werden privates Sicherheitspersonal und Videoüberwachung eingesetzt. Zusätzlich soll die Gestaltung von Räumen unter Sicherheitsaspekten normkonformes Verhalten unterstützen und Abweichung unterbinden. Die raumpsychologischen Mittel dazu werden später in dieser Arbeit ausgeführt.

- *Grundlegender Wandel der Logik politischer und staatlicher Sicherheitsproduktion:* „Wohlfahrtsstaatliches Strafen“ wird ersetzt durch eine neue Punitivität, die sich wieder vermehrt der Vergeltung zuwendet. Im Mittelpunkt der Strafrechtspolitik steht nicht mehr die psycho-soziale Behandlung der Täter, sondern der Schutz für potentielle Opfer, gleichsam der Gesellschaftsschutz. Andererseits zeigt die alt bewährte Staatssicherheit Auflösungstendenzen in einem solidarischen Europa, während die individuelle Sicherheit der BürgerInnen in den Vordergrund rückt.
- *Entwicklung einer Kontrollkultur der gleichzeitigen Moralisierung und Entmoralisierung abweichenden Verhaltens:* Eine Moralisierung abweichenden Verhaltens zeigt sich in „öffentlicher Empörung, moralischen Paniken und der Produktion von Sündenböcken sowie Forderungen nach exkludierender Punitivität (Groenemeyer 2010, S. 15)“. Gleichzeitig konstatieren Kriminologen Tendenzen der Thematisierung von Devianz als „(sozial-)technisch zu bewältigendes und entmoralisierendes, tendenziell versicherbares Risiko (ebd. S. 15)“, bei dem der Täter gegenüber der *Tat* oder dem *Schaden für das Opfer* in den Hintergrund rückt.
- *Ablösung der Konstruktion der Sicherheitsbedrohungen von Kriminalität:* Das Zauberwort heißt „comprehensive security“, und meint die Pluralisierung von Sicherheitsbedrohungen einschließlich der nationalen (militärischen) Sicherheit, der ökonomischen Sicherheit, der ökologischen Sicherheit sowie der persönlichen Sicherheit – kurz: eine Verunsicherung in allen Lebenslagen und allen Dimensionen der Gesellschaft. Was im Englischen so schön in zwei Begriffe gekleidet wird (safety und security) wird in diesem Begriff vereint: Kriminalität ist nur eine Bedrohung unter vielen. Gleichzeitig werden ursprünglich soziale Themen wie Migration, Arbeitslosigkeit, Schuleschwänzen und Obdachlosigkeit als Sicherheitsprobleme der modernen Gesellschaft kriminalisiert.

Anders als in vormodernen Zeitepochen beunruhigt uns jedoch nicht (nur) die Gefahr die von Naturkatastrophen wie Vulkanausbrüchen, Überschwemmungen und Erdbeben ausgeht, sondern es sind Gefahren die wir als Nebenwirkungen der modernen Technologieentwicklung in Kauf nehmen. Diesen Gedanken hat Ulrich Beck in seinem bahnbrechenden Buch „Risikogesellschaft“ (Beck 1986) deutlich dargelegt. Der Unterschied zu früher liegt dabei vor allem im Umgang mit Gefahren: Während frühere Gesellschaften an der Macht der Magie und an religiösen Riten festhielten oder einfach das Schicksal für Ereignisse verantwortlich machten, wird heute mit den selbst produzierten Gefahren anders umgegangen: Sie werden kalkuliert und in Risiko umgewandelt. Die Sicherheit der Moderne wird entmystifiziert, Unsicherheiten werden nicht länger als externe Bedrohungen, sondern als beherrschbare Risiken konstruiert. Das *Prinzip der rationalen Kalkulation* hat bereits der Soziologe Max Weber am Beginn des 20. Jahrhunderts erkannt (Weber 1980; orig. 1922): Das traditionelle Sicherheitsverständnis der Moderne geht davon aus, dass die Bedrohung abnimmt, je größer der Aufwand bei den Schutzmaßnahmen ist. Der Trugschluss, dem die meisten Sicherheitsforscher in ihrer technischen Risikoabschätzung unterliegen ist, dass Sicherheit lediglich eine Funktion von wissenschaftlichem Fortschritt sei, und es nur eine Frage der Zeit ist, oder der für die Forschung zur Sicherheitstechnologie zur Verfügung gestellten finanziellen Mittel, bis wir alle Risiken perfekt beherrschen können. Der „additiven Sicherheitslogik“ zufolge ist Sicherheit abhängig von der Naturbeherrschung und der Verwissenschaftlichung des Risikos (vgl. Bonß 1997). Ich werde im Folgenden aus dieser umfangreichen gesellschaftsdiagnostischen Beschreibung einen Aspekt herausgreifen und vertiefen: Den Aspekt der Neukonfiguration öffentlicher Räume im Dienst der Sicherheit. Dazu bediene ich mich einer soziologischen Analyse – der *Sozialen Morphologie*, die sich insbesondere dann eignet, wenn es um den materiellen Ausdruck sozialer Tatsachen geht.

2 Soziale Morphologie: Die Materiellen Formen des Sozialen

Die „Soziale Morphologie“ wurde als theoretisches Programm zuerst von Émile Durkheim, einem der Gründerväter der Soziologie im 19. Jahrhundert, entworfen und von Marcel Mauss und Maurice Halbwachs weiter ausgearbeitet. In seinen „Regeln der Soziologischen Methode“ (1895; 1961) betont Durkheim ausdrücklich, dass das Soziale nicht nur aus sozialem Handeln, Kommunikation und Symbolen besteht. Vielmehr manifestiert sich Gesellschaft auch im Materiellen, in Verkehrsmitteln, in Kleidung, in Maschinen, Sportstätten – und allgemein gesprochen: in Räumen. Das Programm der Sozialen Morphologie wird somit interessant für die Architektursoziologie, indem das Soziale sichtbare und greifbare Gestalt annimmt, und es wird heute insbesondere interessant für die Kriminologie, indem ein theoretisches gesellschaftspolitisches Konstrukt wie die „Sicherheitsgesellschaft“ in eine materielle Form gegossen wird.

Ich werde zunächst in einem kurzen Exkurs das Programm der Sozialen Morphologie darstellen, und dieses danach am gesellschaftlichen Phänomen der Sicherheitsgesellschaft überprüfen. Es soll gezeigt werden, dass die Sicherheitsgesellschaft nicht einfach nur ein Gedankengebilde der Kriminologen ist, sondern sich am materiellen Substrat der Stadt ablesen lässt.

Soziale Morphologie war für Durkheim ein Programm zur Analyse von gesellschaftlichen Tatbeständen im Übergang von vormodernen, homogenen, mechanischen Gesellschaften zu heterogenen, organischen, durch Spezialisierung und Arbeitsteilung charakterisierten Gesellschaftsformen. Soziale Morphologie nannte Durkheim die Erforschung der materiellen Gestalt von Gesellschaften, jene physische Natur der Gesellschaft, die sich zunächst durch Anzahl, Dichte, Ausdehnung, Bewegung manifestiert. All das kann zwar auch die Demografie leisten, jedoch geht das Programm der Sozialen Morphologie darüber hinaus. Sie geht davon aus, dass die demografische Gestalt von Gesellschaft nicht zufällig in die Landschaft gesetzt ist, und dabei wie aus der Vogelperspektive betrachtet die Gestalt von Dörfern, Städten und Metropolen annimmt. Soziale Morphologie beschreibt uns für eine Gesellschaft typische Sachverhalte, die auf bestimmte kulturelle Entwicklungen, religiöse Werthaltungen, soziale Gewohnheiten und Überzeugungen zurück zu führen sind. Maurice Halbwachs, der die Tradition der Sozialen Morphologie fortgeschrieben hat, bemerkt dazu: „Institutionen sind nicht einfach nur Gedankengebilde; sie müssen auf die Erde gebracht werden, ganz mit Stofflichem beschwert, menschlichem Stoff und unbelebtem Stoff, mit Lebewesen aus Fleisch und Blut, mit Bauwerken, Häusern, Plätzen, dem Gewicht des Raumes. All diese Dinge gehören dazu, es sind Gestaltungen im Raum, die man beschreiben kann, zeichnen, messen und wägen, deren Teile man zählen, deren Ausrichtung, deren Veränderung man erkennen, deren Vergrößerung, deren Verkleinerung man sehen kann. In genau diesem Sinne besitzen dann alle Einrichtungen des sozialen Lebens auch materielle Formen (Halbwachs, 1938; 2002, S. 15-16)“.

An einem konkreten Fall lässt sich der Zusammenhang zwischen Raumstrukturen und kulturellen Lebensweisen verdeutlichen. Im Jahr 1906 hat Marcel Mauss „Eine Studie zur Sozialen Morphologie“ veröffentlicht, in der er den jahreszeitlichen Wandel der Eskimogesellschaften eingehend untersuchte. Mauss stellte fest, dass das kollektive Leben der Eskimovölker im Sommer und im Winter sehr unterschiedlich ist: Während Familien im Sommer zerstreut und autonom in kleinen Rundzelten lebten, wohnten dieselben Familien im Winter viele Kilometer entfernt in Kollektiven in großen Langhäusern zusammen. Mit dem Wechsel der Organisation des Wohnens, der ja möglicherweise klimatisch bedingt ist und durch die Nahrungsverfügbarkeit erklärt werden kann, konnte Mauss aber auch einen signifikanten Wandel der kulturellen Gewohnheiten nachweisen: „Die Religion der Eskimos durchläuft denselben Rhythmus wie ihre Organisation.

Es gibt bei ihnen sozusagen eine Sommerreligion und eine Winterreligion, oder vielmehr gibt es im Sommer keine Religion. Der einzige Kult, der dann praktiziert wird, ist der private, häusliche: es reduziert sich alles auf Geburtsriten und Todesriten, sowie auf die Beachtung einiger Verbote. Alle Mythen, die … im Winter das Bewusstsein der Eskimos erfüllen, scheinen während des Sommers vergessen. … Demgegenüber lebt die Wintersiedlung sozusagen in einem Zustand fortwährender religiöser Überspanntheit (Mauss 1906; 2010, S. 242f.)". Noch deutlichere Auswirkungen hat der jahreszeitliche Wandel der Lebensform auf das Rechtsleben, also auf die Regelung von Rechten und Pflichten im Kollektiv. Das „Recht des Sommers" unterscheidet sich grundlegend vom „Recht des Winters". Das hat Auswirkungen auf das Familienleben, das im Sommer eher patriarchalisch organisiert ist, und im Winter clan-artig in Kommunen ausgeprägt ist, was wiederum Folgen für Verwandtschaftsverhältnisse und Sexualpraktiken hat. Außerdem ist das Eigentumsrecht im Sommer auf die Kernfamilie ausgerichtet, wobei bestimmte Güter wie Waffen den Männern und alle Werkzeuge des Haushalts den Frauen gehören, während das Eigentumsrecht im Winter ein kollektives ist, bei dem der Besitz auf alle Hausbewohner gleichzeitig ausgedehnt wird – alles gehört allen.

Obwohl das Beispiel der doppelten Sozialen Morphologie der Eskimogesellschaften auf den ersten Blick wohl eine Besonderheit darstellt, finden wir Parallelen insbesondere in der Spätmoderne in Europa: „Multilokalen Lebensformen" gewinnen zunehmend an Bedeutung: Seit den frühen 1970er Jahren verbringen Städter jedes Wochenende im Schrebergarten am Stadtrand, oder im Wochenendhaus am Land. Wer es sich leisten kann, „überwintert" im Süden auf einer Insel im Mittelmeer. Doch Multilokalität ist nicht nur ein Phänomen der Reichen, wenn man bedenkt, dass auch Handwerker aus östlichen Nachbarländern als „Gastarbeiter" über die Grenze nach Österreich kommen um auf Baustellen zu arbeiten, und das Wochenende wieder zu Hause bei der Familie verbringen. Multilokalität erfordert bestimmte Infrastruktur, und damit entsteht in Grenzregionen, in Kleingemeinden, am Stadtrand und in der Großstadt eine speziell auf die jeweiligen Bedürfnisse angepasste Morphologie von ökonomischen Versorgungseinrichtungen, sozialen Diensten und Freizeiteinrichtungen. Das soziale Phänomen der Multilokalität drückt den Regionen ihren Stempel auf.

Wenden wir uns nun wieder dem sozialen Phänomen der „Sicherheitsgesellschaft" zu, das ich eingangs beschrieben habe. Meine These lautet, dass in gleichem Maße wie es eine religiöse Morphologie, eine ökonomische Morphologie, eine Morphologie der Mobilität, eine Morphologie der Multilokalität usw. gibt, auch eine Morphologie der Sicherheitsgesellschaft auszumachen ist. Diese soll im Anschluss in Grundzügen nachgezeichnet werden.

3 Die Materialisierung der Sicherheitsgesellschaft in Architektur und Städtebau

3.1 Defensive Design

„Defensive Design“ ist so alt wie die zivilisierte Menschheit. Seit dem Ende des Nomadentums und mit dem Beginn der Sesshaftigkeit hat Eigentum an Wert gewonnen. Landwirtschaftliche Produkte, Werkzeuge und Wohnstätten, musste nicht nur vor Umwelteinflüssen und Tieren geschützt werden, sondern auch gegenüber Räubern und Plünderern. Gleichsam wurde seither Territorium, ob nun als Privatbesitz, als Siedlung, als Fürstentum oder als Staatsgebiet, in verschiedenen Formen gekennzeichnet und verteidigt. Die Grenzen der Agora von Athen wurden ca. 600 vor Christus abgesteckt, als man Grenzsteine mit der Inschrift „Ich bin die Grenze der Agora“ setzte. Die frühe „Verteidigungsarchitektur“ des Mittelalters war geprägt durch eine Kombination von massiven Stadtmauern, Gräben und Flüssen, um Feinde abzuwehren. In Wien wurde beispielsweise nach der Abwehr der ersten Türkenbelagerung 1529 die mittelalterliche Befestigungsanlage modernisiert, indem 12 Basteien mit Stadttoren sternförmig errichtet wurden. Ein ca. 500 Meter breiter Raum vor der Stadtmauer, das Glacis, diente als Schussfeld und durfte nicht verbaut werden. Nur allmählich öffnete sich die „Altstadt“ gegenüber den Vororten und Vorstädten, die Stadtmauern verloren ihre Verteidigungsfunktion und wurden durch symbolische, aber politisch umso wirksamere, Landesgrenzen ersetzt. Man könnte sagen: Die Morphologie der Stadtgrenze wird unscheinbar und verschwimmt. Mit der Auflösung der Habsburger-Monarchie und der zunehmenden Bedeutung der Nationalstaaten haben sich physische Grenzen jedoch nur verschoben. Im 20. Jahrhundert haben militärische Anlagen an den Staatsgrenzen die Funktion der städtischen Festungsanlagen übernommen. Dabei wurde noch auf einen Landstreifen zwischen den Ländern Wert gelegt, der als „Niemandsland“ zwischen den Staaten als Pufferzone für die Menschen in benachbarten Territorien zusätzlich Schutz bieten sollte. Die Kontrollrituale an den Grenzübergängen sind uns noch gut in Erinnerung, und wir werden regelmäßig zu bestimmten „Hochrisiko-Ereignissen“ wie Fußballeuropameisterschaften oder Weltwirtschaftsforen wieder damit konfrontiert. Nichts desto trotz hat sich die Risikolage in Europa dahingehend verändert, dass zwischenstaatliche Konflikte nicht mehr militärisch ausgetragen werden, sondern in der Zeit nach dem Kalten Krieg diplomatische Lösungen angestrebt werden. Internationale Allianzen zur Friedenssicherung haben die fragile Machtbalance der Nachkriegszeit in Europa abgelöst, und nationale Armeen haben neue Aufgaben im Katastrophenschutz übernommen. Damit hat sich aber auch die Risikowahrnehmung der Bevölkerung verändert: Vorstellungen von Unsicherheit in Europa beziehen sich nicht mehr vorrangig auf militärische Konflikte. Überhaupt ist der Feind nicht mehr klar auszumachen, wenngleich verschiedene Medien immer noch an einigen konkreten Feindbildern festhalten. Unsicherheit wird zum diffusen Gefühl, das vielfältig in allen Lebenslagen erlebt wird.

Dieser Wandel ist auch in der Rhetorik zum Sicherheitsbegriff ablesbar: „Nationale Sicherheit“ wurde abgelöst durch „Human Security“. Im United Nations Development Programme (UNDP, 1994) wird “Human Security” zum allumfassenden Konzept der Politik: „Human security shall be addressed by political, social, environmental, economic, and cultural programmes designed collectively to furnish the building blocks of survival, livelihood and dignity (UNDP, 1994).[53]

Kritiker haben bezüglich dieser Ausdehnung des Sicherheitsbegriffs auf ökonomische, soziale, gesundheits- und bildungspolitische Fragen der Gesellschaft Bedenken geäußert, weil damit soziale Probleme kriminalisiert würden (vgl. Zedner 2009). Unaufhaltsam wird Sicherheit zum Leitkonzept hochstilisiert, nur eben nicht mehr nur in der Landesverteidigung, sondern in allen zivilen Belangen. Risikokalkulation und die Produktion von Sicherheit sind zum entscheidenden Wirtschaftsfaktor geworden, von dem sowohl die Sicherheitsindustrie mit ihren mechanischen, elektronischen und EDV-gestützten Frühwarnsystemen profitiert, als auch die Wissenschaft mit ihrer Krisen-, Katastrophen- und Evakuierungsforschung.

Die Morphologie der Sicherheit, also der physische Ausdruck eines bestimmten sozialen Phänomens, hat sich von den Staatsgrenzen in das Landesinnere verlagert. Nicht mehr das Volk, die Nation oder der Staat stehen im Mittelpunkt, sondern der Schutz des Einzelnen ist nun die Hauptsache der Sicherheitspolitik. Das Ziel der Kriminalprävention hat sich außerdem verlagert vom Justizsystem zu einem Präventionssystem der Wirtschaft und Technik. Der Generalprävention mittels Abschreckung durch Strafen und der Spezialprävention durch Sanktionierung, Rehabilitation und Reintegration von Rechtsbrechern wird nun ein System zur Seite gestellt, in dem Objektschutz und Personenschutz im Vordergrund stehen und in dem Tatgelegenheiten vermieden werden sollen. Diesem Präventionsverständnis liegen zwei Prämissen zugrunde:

- *Routine Activity Theory:* Tatgelegenheiten ergeben sich aus der Alltagsroutine durch das Zusammentreffen von drei Komponenten: Einem motivierten Täter, einem geeigneten Ziel oder Opfer, und die Abwesenheit von Beobachtern (Felson 2002).
- *Rational Choice Theory:* Täter sind rationale Nutzenmaximierer, die den eigenen Aufwand für eine Straftat dem Gewinn gegenüber stellen. Die unmittelbare Situation ist die Summe der Informationen aus der Umgebung, die ein motivierter Täter für seine Entscheidung vor der Tat heranzieht (Clarke und Cornish 1986).

53 Im Hinweis auf den Text heißt es: „The 1994 Report introduces a new concept of human security, which equates security with people rather than territories, with development rather than arms. It examines both the national and the global concerns of human security” http://hdr.undp.org/en/reports/global/hdr1994/.

Aufbauend auf der Routine Activity Theory (Felson 2002) und der Rational Choice Theory (Clarke und Cornish 1986) tritt ein Präventionsmodell in den Vordergrund, das auf rationale Plantäter zugeschnitten ist: Täter wollen unbeobachtet sein, unerkannt bleiben und nach der Tat schnell flüchten können. Dementsprechend sind der Tataufwand zu erhöhen, das Entdeckungsrisiko zu erhöhen und der Tatertrag zu verringern.

Ich werde in der Folge zeigen, welche städtebauliche und architektonische Gestalt das Streben nach innerer Sicherheit in unserer Gesellschaft angenommen hat. Dabei kommen nicht nur mechanische und elektronische Sicherheitsprodukte zur Anwendung. Die Produktion von Sicherheit bedient sich der Raumpsychologie, um Täter von ihrem Vorhaben abzuhalten, und subjektives Sicherheitsgefühl zu stärken.

3.2 Sozial-räumliche (situative) Kriminalprävention

Die Sicherheitsgesellschaft hat auch in der Architektur ihre eigenen Werkzeuge zur Kriminalprävention entwickelt. Diese Werkzeuge zeichnen sich dadurch aus, dass sie nicht an individuellen oder sozialpolitischen Bedingungen der Kriminalität ansetzen, beispielsweise an Sozialisationsdefiziten von Jugendlichen oder Arbeitslosigkeit und fehlendem Wohlstand, sondern die *unmittelbare Situation der Straftat* in den Vordergrund stellen. Daraus ergibt sich eine Vielfalt von Möglichkeiten die im Fachbegriff *„Situative Kriminalprävention“* zusammengefasst werden. „Situative Kriminalprävention“ wird im englischsprachigen Raum unter verschiedenen Begriffen diskutiert: „Design Against Crime“ und „Designing Out Crime“ versprechen, mit Hilfe von Planungs- und Gestaltungsmaßnahmen in städtischen Lebensräumen Kriminalität entgegenwirken zu können. Für „Crime Prevention Through Environmental Design“ wurde mit dem Akronym CPTED (gesprochen: sep-ted) ein Kriminalpräventionsansatz gefunden, der aus der Architekturkritik von Jane Jacobs, Oscar Nerwman und C. Ray Jeffery in den USA der 1970er Jahre in die Britische Kriminologie der 1990er Jahre übernommen wurde (J. Jacobs 1961; O. Newman 1972; C.R. Jeffery 1972; R.V. Clarke 1992; T. Crowe 2000).

„Situative Kriminalprävention“ verfolgt zwei Hauptziele:
1. Die Veränderung der Tatgelegenheit für Täter in verschiedenen sozial-räumlichen Situationen
2. Die Steigerung der Raumqualität zur Verbesserung der subjektiven Sicherheit

Obwohl diese Ziele sehr unterschiedliche Ansprüche darstellen, werden sie in den Empfehlungen gemeinsam gedacht und in den Maßnahmen vereint. Jedoch sind Tatgelegenheiten wesentlich komplexer als die Überwindung von technischen Hindernissen beim Wohnungseinbruch.

Tatgelegenheiten setzen sich aus einer Summe von sozialen Bedingungen zusammen, die sich aus der Komplexität aus *gebauten Strukturen*, *sozialen Strukturen*, *Infrastrukturen* und *Raummanagement* ergeben. Ob eine Situation für eine Straftat in den Augen eines Täters „günstig" erscheint, hängt mit der bautechnischen Gestaltung, mit der durch die Nutzung bedingten sozialen Kontrolle und mit einem funktionierenden Ordnungsmanagement zusammen. Situative Kriminalprävention in der Sicherheitsgesellschaft funktioniert nicht allein über Kontrolle und Überwachung, sondern über soziale Ordnung, über die Verdeutlichung von Verhaltensnormen und über die gezielte Herstellung von Raumatmosphäre.

3.2.1 Die Komplexität der Tatgelegenheit

Standards und Normen zur Berücksichtigung von kriminalpräventiven Aspekten in der Bauindustrie waren lange Zeit auf Technologieentwicklung beschränkt: Mechanische und elektronische Produkte zum Objektschutz, sowie Software-Entwicklungen zur Erkennung von kriminellen Verhaltensweisen, werden auch weiterhin gezielt beworben, um NutzerInnen von Gebäuden und Infrastrukturen größtmöglichen Schutz vor Verbrechen anzubieten. Genormt werden Qualitätssicherungsmerkmale für Alarmanlagen, Schlösser, Schutzbeschläge, Sicherheitsfenster, Sicherheitstüren und Sicherheitssonderverglasung, ebenso wie für Wertbehältnisse und Tresorräume.

Neben der Sicherheitstechnologie, die einem motivierten Täter die Arbeit erschwert, beeinflussen auch andere Raummerkmale die Gesamtsituation: Die *Bauform* (weite oder enge Räume, hohe oder niedrige Räume, Gebäudestrukturen etc.), *Lichtverhältnisse* (natürliches Licht, künstliches Licht, gleichmäßige Lichtverteilung, Spots etc.), *Materialien* (glatte Fliesen, Betonmauerwerk, Ziegel, etc.), *Farben* (warme Farben, kalte Farben, dunkel, hell), *Gerüche* (unangenehme Gerüche, Luftqualität etc.) und *Zugluft* (Düseneffekt) sind Merkmale die nicht nur einen Täter beeinflussen, sondern insbesondere auch das Sicherheitsgefühl der Anrainer und Passanten nachhaltig bestimmen. Die raumpsychologische Wirkung lässt sich bewusst und gezielt steuern, indem diese Elemente in der Planung berücksichtigt werden. Bei Vernachlässigung lassen sich jedoch Verwahrlosungstendenzen feststellen, die in einer Abwärtsspirale zu physischem und sozialem Niedergang eines Stadtteils führen können (Wilson und Kelling 1982). Zusammen mit Alarmanlagen, Sicherheitstüren und Sicherheitsschlössern bilden die physischen Raummerkmale den materiellen Rahmen für Tatgelegenheitssituationen.

Soziales Leben

Tatgelegenheitsstrukturen lassen sich nicht alleine durch materielle Raumelemente beschreiben. Die Verteidiger der Situativen Kriminalprävention geben uns zu verstehen, dass jeder physische Raum gleichzeitig auch Sozialraum ist, und dass eine Reihe von sozialen Komponenten zur Situation auf Plätzen, Straßen und in Parks beitragen. Dazu zählen beispielsweise die demografische Komposition in einem Stadtviertel und Segregation bzw. die soziale Durchmischung von Bevölkerungsschichten. Nur durch die Integration von Vielfalt sind separate Parallelkulturen zu vermeiden, und nur durch regelmäßige soziale Kontakte können Vorurteile abgebaut und im Gegenzug sozialer Zusammenhalt in einer Gemeinschaft ermöglicht werden. Ein nachbarschaftliches Gemeinwesen beruht auf breitem Konsens über Gemeinsamkeiten, das können Kinder sein, die zusammen im Park spielen, das können aber auch kleine Interessensgemeinschaften sein, die ähnliche Freizeitinteressen haben. Erst dann kann von den Anrainern nachbarschaftliche Leistung im Sinne von sozialem Kapital erwartet werden. Zumindest eines haben die Menschen in einem Wohngebiet gemeinsam: die Nachbarschaft. Der soziale Zusammenhalt in der Nachbarschaft wird dann forciert, wenn sich die Menschen mit „ihrem“ Wohnviertel verbunden fühlen. Die Wahrnehmung einer bestimmten Identität, die architektonisch pointiert werden kann, ist die Grundlage für erfolgreiche individuelle Identifikation mit dem Wohnumfeld einerseits und für Kollektivbewußtsein andererseits. Aus der Perspektive der Kriminalprävention wird betont, dass auch motivierte Täter bei der Vorbereitung auf eine Straftat ein Gefühl für nachbarschaftliches Kollektivbewußtsein haben, und erkennen, ob sie in einem Gebiet agieren, das sich durch besondere Anonymität auszeichnet, oder das durch informelle soziale Kontrolle charakterisiert ist. Dieses Gefühl der nachbarschaftlichen Verantwortlichkeit, das empirisch nur sehr schwer erfasst und nachgewiesen werden kann, wurde von dem Architekt Oscar Newman in den 1970er Jahren in seinem Begriff „Defensible Space“ als wesentliche Komponente der Kriminalprävention durch Stadtplanung und Design ausgewiesen: Wer sich mit seinem Stadtviertel emotional verbunden fühlt, ist eher bereit die Ordnung in diesem Viertel zu verteidigen. Dieser „Lokalpatriotismus“ und die entsprechende emotionale Verbundenheit mit dem Territorium ist das Ziel architektonischer Planung und Gestaltung.

Funktionale Infrastrukturen

Die Anwesenheit und das Verhalten von Menschen im öffentlichen Raum werden wesentlich vom infrastrukturellen Angebot bestimmt. Das Angebot umfasst Verkehrsmittel und Haltestellen, Lebensmittelgeschäfte, Kleidungs- und Schuhgeschäfte, Ärzte und Apotheken, Frisöre, Bäckereien, religiöse Einrichtungen, Schulen, Museen, Kindergärten, Spielplätze für Kleinkinder, für Schulkinder und Jugendeinrichtungen, Wettbüros, Lokale, Fast-Food-Restaurants, Bauernmärkte, Elektronikhandel, Blumenhandlungen und Vieles mehr.

Die funktionale Vielfalt bringt auch vielfältiges Publikum und Belebung zu bestimmten Tages- und Nachtzeiten, während an monofunktionalen Orten wie Wohnsiedlungen, Gewerbeparks und Einkaufszentren einzelne Zielgruppen dominieren. Belebung ist planbar, und ebenso sind Isolation, Verwahrlosung und der Eindruck ein Viertel sei „ausgestorben“ die Folge von infrastrukturellen Begebenheiten. Monofunktionale Reihenhaussiedlungen am Stadtrand („Suburbs“) sind oft von einem „moralischen Minimalismus“ (Baumgartner, 1988) geprägt, wo Anonymität, geringe soziale Kohäsion und minimale soziale Kontakte eine soziale Kontrolle reduzieren. In diesen Siedlungen fährt man grundsätzlich mit dem Auto, kaum jemand geht zu Fuß, weil es bis zur nächsten Infrastruktureinrichtung zu weit ist. Ohne einem wertkonservativem Kommunitarismus (Etzioni, 1998) zu verfallen, fordern Vertreter dieses Ansatzes, dass zumindest die Gelegenheit für zufällige persönliche Begegnungen in der infrastrukturellen Planung zu berücksichtigen sei.

Das Management der Ordnung

Die Planung kann für Ordnung nicht alleine verantwortlich gemacht werden. Orte werden nicht immer so genutzt, wie das die Planung vorgesehen hat, denn gesellschaftliches Leben ist eben dynamisch und nicht statisch. Ein Aspekt der Sicherheit ist dabei die Gewissheit in Bezug auf das Erwartbare, das Bekannte, das Gewohnte und das Normale. Um ein gewisses Ordnungsniveau aufrecht zu erhalten, sind konkrete Maßnahmen erforderlich, die das soziale Leben funktionieren“ lassen. Zu diesen Routine-Arbeiten zählen zunächst alle Aktivitäten zur Erhaltung, Sanierung, Entsorgung, Zulieferung, Reinigung und Reparatur im öffentlichen Raum. Darüber hinaus ist aber auch ein Management für den flüssigen Verkehrsablauf von Bedeutung, also die Abstimmung der Fahrpläne der Verkehrsmittel aufeinander und auf Öffnungszeiten und Sperrstunden bzw. auf Zeitpunkte, zu denen erhöhtes Verkehrsaufkommen zu erwarten ist. Beispielsweise können die Verkehrsbetriebe bewusst auf Schulschlusszeiten reagieren, wenn mehrere Schulklassen gleichzeitig auf die Straße strömen. Hier kann mit Hilfe von Ordnungsmanagement Konfliktpotential unterbunden und Eskalation verhindert werden. Der australische Kriminologe Richard Wortley (2008, S. 48ff.) hat den Begriff der „Precipitators of Crime“ in die Diskussion eingebracht, und meint damit die unmittelbaren sozialräumlichen Begebenheiten, die Konflikte auslösen können: Soziales Gedränge, Hitze, Lärm, Frustration durch lange Warteschlangen, usw. können eine Eskalation von Gewalt unterstützen. Diese sozialräumliche Atmosphäre ist in einem Ordnungsmanagement zu berücksichtigen. Die Verantwortlichkeit für dieses umfangreiche urbane Facility Management obliegt nicht allein den Überwachungs- und Exekutivorganen, sondern einem komplexen System von Ordnungseinrichtungen in der Regionalverwaltung, das sozialräumliche Dynamiken erkennen und steuern soll.

3.3 Von der Raumpsychologie zur Raumsoziologie

Wir haben gesehen, dass man mit bewusst eingesetzten raumpsychologischen Akzenten die Atmosphäre an städtischen Orten dahin gehend manipulieren kann, dass der Raum einerseits wenig Möglichkeiten für motivierte Straftäter bietet, und andererseits den Menschen die diese Räume nutzen ein angenehmes, vertrautes und damit sicheres Gefühl vermittelt. Alle genannten Maßnahmen – physische Raumgestaltung, infrastrukturelle Widmung (Funktionalität), soziale Belebung und Demografie, Ordnungsmanagement – können die Mikrostrukturen einer sozialräumlichen Situation beeinflussen. Das ist jedoch nur die halbe Wahrheit, denn alle diese positiven Ambitionen vergessen, dass eine Raumkosmetik dieser Art gegen makro-soziale Strukturen nur schwer ankommt. Dabei sind es politische Entscheidungen, die nicht direkt mit Raumplanung oder Städtebau zu tun haben, aber dennoch sich tief in das soziale Gefüge einer Gesellschaft einbrennen, und ebenfalls in der Morphologie der Städte hervor treten. Soziale Trends haben Konsequenzen für die Gestalt unserer Städte, und letztlich auch für Tatgelegenheiten. Diese „Nebeneffekte“ sind bislang im Ansatz der „Situativen Kriminalprävention“ unbemerkt geblieben. Dazu möchte ich nur einige Beispiele anführen.

3.3.1 Konsum

Der historische Wandel von ökonomischen Strukturen, insbesondere die Herausbildung einer konsumorientierten Gesellschaft hat immer neue Tatgelegenheiten gebracht. Marktplätze, Einzelhandel, Einkaufsstraßen, Kaufhäuser, Shopping Center, Gewerbeparks – alle bieten unterschiedliche Kontrollstrukturen, die es Dieben bzw. Einbrechern mehr oder weniger leicht machen. Beispielsweise wird in Einkaufszentren die fehlende soziale (informelle) Kontrolle ersetzt durch Überwachung mittels privater Sicherheitsdienste, die durch möglichst zuverlässige Sicherheitstechnologie unterstützt werden. Dafür werden Räumlichkeiten vorgesehen, die als Sicherheitszentralen eingerichtet werden. Die Ursache für zunehmende Diebstähle ist jedoch nicht die hohe Anzahl von Kleptomanen, auch nicht die mangelnde Kontrolle des Sicherheitspersonals. Die Ursache liegt in der unpersönlichen, anonymen Struktur des Konsums am Stadtrand, im Gegensatz zu den kleinen persönlichen Läden wie wir sie in dörflichen Strukturen, aber auch in stark integrierten Stadtteilen finden. Die Form des Konsums wirkt auf Legalverhalten. Vielen Betreibern von Einkaufszentren sind Jugendliche ein Dorn im Auge, weil diese die Eingangshallen als Spielplatz zum Skateboarden, oder einfach nur als sozialen Treffpunkt nutzen. In den Einkaufsstraßen und Fußgängerzonen sind Jugendkulturen selbstverständlich gewesen. Jetzt werden diese vertrieben, weil sie nicht dem gewünschten kaufkräftigen Publikum angehören, und den Konsum stören. Ein ähnliches Phänomen der Verdrängung finden wir im Fall von Obdachlosen auf Bahnhöfen. Es ist die makro-soziale Struktur einer Gesellschaft, die für Unordnung und Konflikte verantwortlich ist.

3.3.2 Bildung

Auch die strukturelle Transformation von Bildungseinrichtungen hat ihre Folgen: Waren früher Schulen vereinzelt in der Stadt „verstreut“, so werden heute mehrere Schulen zu Schulzentren zusammen gefasst, und bilden einen Schulcampus. Das mag wohl aus Bildungspolitischer Sicht rational überlegt sein, hat jedoch Konsequenzen auf die Nutzungsstruktur in diesem Stadtteil, denn in den Ferien steht der Campus für mehrere Wochen leer. Die Aufrüstung der Schulen mit EDVGeräten (Computer, Server, Drucker, Software) stellt zusätzlich Anreize für Einbrüche in Schulen dar, die durch ihre Baustruktur nur mit hohem technischem Überwachungsaufwand geschützt werden können. Gleiches gilt für Universitäten, die als Campus-Universitäten am Stadtrand geschlossene Enklaven bilden, in denen soziale Heterogenität (Senioren, Kinder, Migranten, Arbeiterschichten) unterbunden wird, während gleichzeitig der Stadt die Studentenkultur entzogen wird. Städte wie Tübingen, Ljubljana, Krakau und Utrecht wären ohne Studenten leblos und leer. Die Ursache für Einbrüche in Schulen und Universitäten mit Campusstruktur ist nicht die mangelnde Überwachung, sondern die städtebauliche Form aufgrund bildungspolitischer Entscheidungen.

3.3.3 Arbeitsplatz

Umgekehrt lassen sich auch positive Beispiele für strukturelle Entwicklungen finden. Die Flexibilisierung von Arbeitszeiten und Arbeitsorten (Tele-Arbeit) hat eine Nutzungsmischung bewirkt. Während in fordistischen Betriebsstrukturen Anwesenheitspflicht mit strengen Zeiterfassungssystemen galten, wird nun zu jeder Zeit und von überall gearbeitet. Das sollte Verkehrsströme entlasten (wenn nicht andere ökonomische Faktoren entgegen wirken) und Wohngebiete tagsüber beleben, da man von zu Hause oder auch von unterwegs Zugang zum Firmennetzwerk hat. Belebte Wohngebiete bieten bessere informelle soziale Kontrolle, und die „Schlafstädte“ am Stadtrand gehören der Vergangenheit an.

4 Schluss

In jeder gesellschaftlichen Epoche, so die These der Sozialen Morphologie, schlägt sich die soziale Organisation im Raum nieder. So wie bei einigen anderen Soziologen später, beispielsweise bei Georg Simmel, Henri Lefebvre und Pierre Bourdieu, sind Raum und Gesellschaft in Durkheim’s Verständnis untrennbar in einem dialektischen Verhältnis miteinander verbunden. Weder der Raum noch Gesellschaft existieren als alleinige Phänomene.

Die Unterscheidungen und Unterteilungen des Raums sind sozialen Ursprungs, also sozial konstruiert. Kasernen, Kirchen, Parlamente, Einkaufszentren sind Ausdruck von militärischen, religiösen, politischen und ökonomischen Institutionen. Umgekehrt sind Raum (und Zeit) verantwortlich für soziale Integration und soziale Ordnung, wie Schroer ausführt: „Raum und Zeit sind dazu da, für Verlässlichkeit, Stabilität und Erwartbarkeit zu sorgen (Schroer 2006, S. 50)“. Wir sehen beispielsweise, dass einzelne Räume bestimmte soziale Verhaltensweisen implizieren: Die Stille in Kirchen, die „Welle“ in Fußballstadien, die Disziplin in Kasernen, das Flanieren in Einkaufsstraßen. Architektur und soziales Leben sind in der Architektursoziologie vereint, sie beschreibt damit die „Gestalt der Gesellschaft (Fischer und Delitz 2009, S. 12)“.

Ich habe versucht, mit Hilfe der besonderen Methode der Sozialen Morphologie den Zusammenhang zwischen Gesellschaftsstrukturen und Raumstrukturen darzustellen, und dabei die Eigenschaften der Spätmoderne zu belegen. Von der Verteidigungsarchitektur des Mittelalters, über Grenzarchitektur bis hin zu den mechanischen, elektronischen und EDV-gestützten Sicherheitstechnologien wurde Sicherheit in verschiedenste Formen gegossen. Die Sicherheitsgesellschaft zeichnet sich jedoch darüber hinaus durch Risikokalkulation und Risikomanagement aus, und dafür wurden neue Präventionsmaßnahmen geschaffen: Raumpsychologische Gestaltungsmerkmale werden genutzt, um die Tatgelegenheiten für Täter zu reduzieren und um den Menschen eine vertraute und sichere Atmosphäre im öffentlichen Raum zu bieten. Für die Weiterentwicklung des Konzepts „Kriminalprävention durch Stadtplanung und Design“ stellt sich allerdings die Frage, wie diese mit gesellschaftspolitischen Entscheidungen und Entwicklungen auf anderen Gebieten wie Bildung, Arbeitsmarkt, Ökonomie in Einklang zu bringen ist, denn jede sozialpolitische Entscheidung hat Konsequenzen für die materielle Umwelt. Es ist dieser transdisziplinäre Zusammenhang, der auch in der Sicherheitspolitik Berücksichtigung finden sollte.

Literatur

- BAUMGARTNER M.P.: The Moral Order of a Suburb. New York, Oxford; Oxford University Press. 1988.
- BECK U.: Risikogesellschaft. Suhrkamp, Frankfurt am Main. 1986.
- BONSS W.: Die gesellschaftliche Konstruktion von Sicherheit. In: Lippert E., Prüfert A., Wachtler G. (Hrsg.): Sicherheit in der unsicheren Gesellschaft. VS Verlag für Sozialwissenschaften. 1997.
- CARRABINE E., LEE M., PLUMMER K., SOUTH N., IGANSKY P.: Criminology: A Sociological Introduction. Routledge. New York. 2004.
- CLARKE R.V. (Hrsg.): Situational Crime Prevention: Successful Case Studies. Albany, New York: Harrow and Heston, Publishers. 1992.
- CLARKE, R.V. and Cornish D.B. (Hrsg.), The Reasoning Criminal: Rational Choice Perspectives on Offending. New York. Springer. 1986.
- CLARKE, R. and ECK J., Crime Analysis for Problem Solvers in 60 Small Steps. Washington DC. Office of Community Oriented Policing Services. US Department of Justice. 2005.
- CROWE T.: Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts. US Crime Prevention Institute. 2nd edition, Boston, Massachusetts: Butterworth-Heinemann. 2000.
- DURKHEIM E.: Die Regeln der soziologischen Methode (frz. 1895). Neuwied / Berlin. Luchterhand. 1961.
- ETZIONI A.: Die Entdeckung des Gemeinwesens – Das Programm des Kommunitarismus. Frankfurt/Main: Fischer Verlag. 1998.
- FELSON, M., Crime and Everyday Life (3rd ed.), Thousand Oaks, Sage Publications. 2002.
- FISCHER J. und DELITZ H.: Die Architektur der Gesellschaft – Theorien für die Architektursoziologie. Transcript Verlag. Bielefeld. 2009
- GARLAND D.: Kultur der Kontrolle – Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Campus Verlag. Frankfurt / New York. 2008; (engl. orig. 2001).
- GROENEMEYER A (Hrsg.): Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. Verlag für Sozialwissenschaften. Wiesbaden. 2010.
- HALBWACHS M.: Soziale Morphologie. Ausgewählte Schriften. Edition discourse. Bd. 4. UvK Verlag. Konstanz. 2002.
- JACOBS J.: The Death and Life of Great American Cities. Random House, New York. 1961.
- JEFFERY C. R.: Crime Prevention Through Environmental Design. Bevery Hills, CA: Sage. 1971.
- KUNZ K.-L.: Kriminologie: Eine Grundlegung. 5. Aufl. UTB. Stuttgart. 2008.
- LEGNARO A.: Konturen der Sicherheitsgesellschaft: Eine polemisch-futurologische Skizze. Leviathan 25/2; S. 271-284. 1997.
- LÖW M.: Raumsoziologie. Frankfurt/Main. Suhrkamp. 1. Aufl. 2001.
- NEWMAN O.: Defensible Space: Crime Prevention Through Urban Design. McMillan, New York. 1972.
- NEWBURN T.: Criminology. Willan. Collumpton. 2007.
- SCHROER M.: Räume, Orte, Grenzen – Auf dem Weg zu einer Soziologie des Raumes. Suhrkamp. Frankfurt/Main. 2006.
- SCHROER M.: Materielle Formen des Sozialen: Die Architektur der Gesellschaft aus der Sicht der Sozialen Morphologie. In: Fischer J. und Delitz H.: Die Architektur der Gesellschaft – Theorien für die Architektursoziologie. Transcript Verlag. Bielefeld. 2009.
- UNDP – United Nations Development Programme: 1994 Report. http://hdr.undp.org/en/reports/global/hdr1994/ (zuletzt aufgerufen Juni 2001). 1994.
- MAUSS M.: Soziologie und Anthropologie. Band 1: Theorie der Magie / Soziale Morphologie. Verlag für Sozialwissenschaften. Berlin. 2010; (Orig. frz. 1906).
- WEBER M.: Wirtschaft und Gesellschaft: Grundriss der Verstehenden Soziologie. Mohr. Tübingen 1980. (original 1922).

- WILSON, J.Q und KELLING, G.L., Broken Windows, in: The Atlantic Monthly; Volume 249, No. 3; pages 29-38. 1982.
- WORTLEY, R., Situational Precipitators of Crime, in: Wortley R. and Mazerolle L. (Hrsg.), Environmental Criminology and Crime Analysis. Willan. Collumpton and Portland. 2008.
- WORTLEY, R. and MAZEROLLE, L. (Hrsg.), Environmental Criminology and Crime Analysis. Willan. Collumpton and Portland. 2008.
- ZINGANEL, M.: Real Crime: Architektur, Stadt & Verbrechen. Edition Selene. Wien. 2003.
- ZEDNER L.: Security. Key Ideas in Criminology Series. Routledge. Abington. 2009.

Internet Links

Netzwerke:

International CPTED Association: http://www.cpted.net/

European Designing Out Crime Network: http://www.e-doca.eu/

European Forum for Urban Safety: http://www.urbansecurity.org/

New Urbanism Network: http://www.newurbanism.org/

Wirtschaftskriminalität, Spionage und der Angriff auf kritische Infrastrukturen werden immer häufiger ein soziopolitisches Thema. Der Bedarf Daten und Informationen zu schützen wird daher immer größer. Das Jahr 2011 ist geprägt von der Omnipräsenz der Themen Cyber Security und Cyber Crime. Mittlerweile ist die gesamte Gesellschaft von den kriminellen Auswüchsen im Netz in irgendeiner Form betroffen, sei es als Individuum, Organisation oder Staat.

Die 9. Sicherheitskonferenz Krems hat das Ziel aktuelle Entwicklungen zum Thema Sicherheit und Kriminalität im Netz aufzuzeigen und die neuesten Forschungsergebnisse zu präsentieren.

Der Architektur in Sicherheitsgesellschaften widmet sich der zweite Schwerpunkt der Konferenz.
Zwei Beiträge behandeln aktuelle Forschungsergebnisse zu baulichen und gestalterischen Formen mit dem Fokus auf Kriminalprävention.

Mit freundlicher Unterstützung

ISBN 978-3-902505-24-8